Anno 2 – N. 30
17 Luglio - 31 Luglio 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it,

Contributors: Bismark.it, Guglielmo Cancelli, darkestsin, Roberto "decOder" Enea, g4i4, Gianluca Ghettini, Milo Cutty, pctips, Gianluca Pomante, SpeedyNT

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

CHI HA PAURA DEL DEFACER CATTIVO?

Stavo pensando di fare un articolo che annuncia, per la giornata di ferragosto, un assalto di massa alle spiagge italiane. Un non bene identificato gruppo di goliardi avrebbe organizzato per quella data una gara di gavettoni: un bagnante colpito con un palloncino pieno d'acqua, un punto; un bagnino, tre punti. Poi, il 16 agosto, potrei dire che in effetti l'attacco è fallito: c'è stato qualche turista colpito qua e la, ma niente di grave.

Più o meno è ciò che è successo in queste settimane con le tanto strombazzate "olimpiadi del defacer": quotidiani e telegiornali hanno speso righe e righe di testo, e preziosi secondi di trasmissione, a parlare di una delirante competizione a base di defacement. In premio: 500 Mbyte di hosting (ma, dico, ci arrivate a capire che nessun vincitore potrebbe ritirare il premio senza automaticamente confessare di essere colpevole di svariati reati? Bah!).

Non fosse per il risalto dato dai media all'evento, nessuno se ne sarebbe accorto. Nonostante il risalto dato alla notizia dai media e da qualche organo istituzionale, italiano e non (risalto che, probabilmente, è stato il vero motivo scatenante di una qualsiasi attività anomala), i siti davvero presi di mira sono stati ben pochi.

I panicked over the Defacement Challenge scare and all I got was this lousy defacement.

THE FUD & HYPE | REALITY CHECK

Simpatica l'iniziativa presa da alcuni siti relativi alla sicurezza: hanno sostituito l'home page con un finto defacement che riportava la scritta: "Mi sono fatto prendere dal panico per la gara dei cracker, e tutto ciò che ho ottenuto è stato questo schifosissimo defacement". Più sotto, molti riportavano un punto di vista un po' più sensato rispetto a questo argomento (magari lo ritrovate ancora su InfoWarrior.org o Kumite.org).

In sintesi, nessuno davvero addentro alla questione "sicurezza" si è preoccupato più che in un giorno normale. Il vero problema è che la maggior parte degli amministratori, nei giorni normali, non si preoccupano per niente, salvo poi correre ai ripari (qualcuno ha persino tirato giù il proprio server per paura di un attacco...), quando i giornali riportano una notizia spazzatura.

Quasi quasi rimpiango i titoli di prima pagina di un quotidiano come "La notte", che in estate diventava davvero irresistibile, o di una rivista come "Cronaca Vera". Cose tipo "Milano invasa dalle rane", "In arrivo le zanzare killer" o "Formosa bionda ruba la pensione a un vecchietta, spacciandosi per operaio del gas, ma prima di andarsene ne costringe il marito rientrato dal cinema porno". Quelle sì che erano notizie.

grand@hackerjournal.it

www.hackerjournal.it

Saremo di nuovo in edicola Giovedì 31 luglio !

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

SIAMO HACKER O CAPORALI?

L'HANC ("HAcker is Not Cracker") è associazione no-profit fondata dai frequentatori del forum di Hj, con lo scopo di tutelare il termine "Hacker", che viene sempre piu spesso usato erroneamente dai mass media per indicare i "pirati informatici", diffondendo cosi un'immagine errata della comunità Hacker. La difesa di questo termine sarà esercitata attraverso la divulgazione dell'Etica Hacker e la sensibilizzazione di stampa, tv e siti internet. Gli obiettivi ambiziosi richiedono una massiccia collaborazione da parte degli utenti. Per ora il forum di discussione lo potete trovare su http://www.hanc.tk in attesa di un dominio "*.org" e della pubblicazione di un manifesto Hacker e dei progetti completi dell'associazione.

Novita!

TESTA IL TUO COMPUTER

Dalla home page di Hackerjournal.it potete accedere a un servizio, realizzato da Bismark, che permette di verificare e migliorare la sicurezza e la velocità del vostro PC e della connessione a Internet. Tra i servizi disponibili (gratis, c'è da chiederlo?) citiamo: Localizzazione IP su una mappa, Scansione falle di sicurezza, controllo velocità di connessione, controllo sicurezza del browser, e tanti altri.

ARTICOLI CALDI...

DktrKranz ha postato sul sito una serie di tre interessanti articoli sull'installazione e configurazione di Windows 2003 Server.

Un altro interessante articolo, anche se un po' più vecchiotto, è una procedura per eliminare lo spyware CyDoor, installato da vari programmi finti freeware. Purtroppo qui non sappiamo a chi fare i complimenti, perché è stato postato in modo anonimo (mannaggia, registratevi e firmate quello che scrivete).

Correte a cercarli nella sezione Articoli di

www.hackerjournal.it

e leggeteveli tutto d'un fiato!

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: at3zzo
pass: rid8

HACKER JOURNAL

mailto:
redazione@hackerjournal.it

CIAO ALESSANDRO!

Gentile redazione Vi scrivo perché una persona davvero speciale è scomparsa il 26/05/03 e io vorrei tanto che fosse ricordato sulla Vs. rivista in quanto per lui questo giornale era come il Vangelo. Alessandro Cavalli 29 anni laureato in Economia e Commercio alla Bocconi e specializzato in crittografia e sistemi di sicurezza, aveva appena realizzato il suo sogno di andare a Roma a lavorare in questo campo, ma il destino "bastardo" ce l'ha portato via...

Era un ragazzo meraviglioso con un sorriso avvolgente ed uno sguardo magnetico (potrei scrivere di lui per 3 uscite della rivista). Purtroppo qualcuno ha deciso che la sua carriera di Hacker dovesse continuare da un'altra parte... Ale una parte di me è 'partita' con te, ti penserò sempre, grazie per avermi voluto bene.

UN'AMICA

Ci uniamo al tuo ricordo, e ci stringiamo attorno a te, agli amici, alla famiglia.

DUE ARTICOLI DI GIORNALE

"Pirati informatici scaricano gratis centinaia di canzoni in formato MP3, per un equivalente di molte migliaia di euro" "Ladri comuni entrano in negozio di articoli musicali e rubano centinaia di CD, per un equivalente di molte migliaia di euro" Qual e' la differenza? Nessuna. Solo, per qualche strano motivo, sentirsi dare del "pirata informatico" fa sentire importanti, mentre farsi dare del "ladro comune" fa sentire offesi. Eppure e' esattamente la stessa cosa. Se una legge non vi piace, fate in modo che venga cambiata, non infrangetela. Altrimenti, un bel giorno qualcuno potrebbe decidere che la legge che gli impedisce di entrare in casa vostra e stabilirsi li' per mangiare e dormire, non e' giusta, e quindi potra' decidere di venire quando vuole e fare quello che vuole in casa vostra.

Comunque, grazie a tutti: io non ho mai scaricato un MP3 in vita mia (a parte quello della sigla di McGyver, per farne la suoneria del mio cellulare), e adesso dovro' pagare una tassa su CD e cassette per ripagare dei vostri furti i produttori/rivenditori.

E grazie anche a tutti per essere saliti sull'autobus senza biglietto: per merito vostro, dall'anno prossimo dovro' pagare un biglietto 1,50 euro invece di 0,77 centesimi, sempre per ripagare i vostri furti. Furti.

Di questo si tratta.

Ladri, non pirati.

LUCA C.

Hai dimenticato l'evasione fiscale, che fa aumentare le tasse, e l'uso dei condizionatori d'aria, che aggrava l'effetto serra (che fa aumentare l'uso dei condizionatori, ripeti ad libitum).

FAR TORNARE VISIBILI I FILE NEL CESTINO

Vorrei dare delle piccole precisazioni sull'articolo "Nascosti nel cestino" di HJ 28 a pag.15.

Avete detto: "Ovviamente, i file sono nascosti alla vista" - e fin qui son daccordo... - "ma perfettamente accessibili a chiunque venga in mente di curiosare nel cestino dal prompt di MS-DOS". FALSO!!! Ai file si può accedere in modo molto più facile, anche da uno che non sa nemmeno cos'è MS-DOS!!!

E' semplice! Basta impostare l'opzione di visualizazzione di tutti i tipi di file (nascosti e di sistema), dal menù Visualizza>Opzioni cartella... ed entrare nella scheda Visualizza.

Così si potrà accedere a tutti i file contenuti nella cartella "recycled". Quindi non c'è tutta questa sicurezza.... E' solo una precisazione! Continuate così che siete mitici!

Cr4$h[87]

Giusta precisazione.

POSTA SICURA IN VACANZA

Salve!Per un po di tempo non avrò a disposizone il mio PC,quindi per controllare le e-mail mi devo recare ad un Internet Point,collegarmi al sito del mio provider e leggere la posta via Web.Tutto questo è sicuro?Voglio dire,non è che un soggetto può recuperare la password(che ho digitato sul sito del mio provider) che si è andata a registrare in qualche meandro di Windows? Quali accortezze mi consiglia-te?

Matteo D.

Come prima cosa, se il servizio Webmail che utilizzi permette l'uso di connessioni sicure (https), sfrutta questa possibilità. Yahoo per esempio lo consente, anche se limitatamente allo scambio delle password (qualcuno potrebbe comunque intercettare le pagine con i messaggi). In alternativa, puoi crearti un'email sul servizio HushMail (www.hushmail.com), che offre appunto la possibilità di consultare una casella di posta in modo assolutamente sicuro. Alla fine, elimina

TRUCCO ANTI DIALER

Voglio segnalare l'esistenza di un piccolo trucchetto che potrebbe far evitare brutte sorprese nella bolletta telefonica di molte famiglie e, chissà, magari salvare la "testa" a qualche utente ancora inesperto sul problema dialer, trattato sul n. 28.

Il trucchetto consiste nel seguire questa stringa C:\Documents and Settings\All Users\Dati applicazioni\Microsoft\Network\Connections\Pbk\rasphone.pbk e impostare il file rasphone.pbk in "sola lettura".

Il trucco funziona solo su OS win2K & XP.

Ho visto questo suggerimento su un forum, in un post di xdesign e ZZZ, e ho pensato di diffondere l'informazione...

badboy84

www.hackerjournal.it

i file temporanei di Internet (cioè pulisci la cache dei browser), e cancella la Cronologia.

☺ Tech Humor ☺

Sai che è tempo di iscriversi all'Anonima Email-dipendenti quando…

- Ti svegli alle 3 di notte per andare in bagno, e ti fermi a controllare l'email mentre torni a letto.
- Dai ai tuoi figli i nomi Eudora, Pegasus e Chicciola.
- Spegni il modem, e hai quel senso di vuoto, come se il tuo amore ti avesse appena lasciato.
- Passi la metà del viaggio aereo con il portatile sulle ginocchia, e tuo figlio nel vano portaoggetti.
- Decidi di stare in università un paio di anni in più, solo per l'accesso a Internet gratuito.
- Usando un word processor, ti ritrovi ad aggiungere "com" o "it" dopo ogni punto.
- Non chiami mai tua madre, perché non ha un modem.
- Controlli la posta. Il programma ti dice che non ci sono nuovi messaggi. Così la controlli di nuovo.
- Ogni volta che sorridi, ruoti la testa di lato di 90 gradi.
- Mentre leggi questo testo, stai pensando a chi inviarlo.

VENDERE SOFTWARE LIBERO

Ho scovato su internet un progetto molto interessante di portale PHP pronto per l'uso, modificabile dall'utente tramite un'interfaccia admin. Si chiama "PHP WebSite" ed è sviluppato dall'Università di Appalache (U.S.A.). Sebbene sia già abbastanza compiuto, soffre ancora di alcuni bug che lo sconsigliano ai non esperti di PHP. Per questo, essendo un Web Designer, mi chiedo se è lecito, dal momento in cui implemento le funzionalità del sito, venderlo ai miei clienti come farei con un qualsiasi altro sito costruito partendo da zero, insieme a un manuale di uso per esempio. Il lavoro dell'Appalachian University è protetto da licenza GPL: mi consente di rivendere il prodotto modificato, così come sono in commercio certe distribuzioni di Linux? I miei potenziali clienti sono persone che in ogni caso non potrebbero beneficiare direttamente di PHP WebSite, per questo dal punto di vista etico mi sembra lecito venderglielo, visto che ho l'intenzione di modificare certe parti del sito, migliorandole se possibile. Qualora arrivassi a una soluzione stabile, mi affretterò naturalmente di inviarla al team che sviluppa il progetto.
Vi sarei grato se poteste darmi qualche informazione sulla legalità del mio progetto, in Italia ma anche all'estero, infatti lavoro anche in Svizzera.

Raphaël J.

Vendere un software protetto da licenza GPL è perfettamente lecito, soprattutto se -come nel tuo caso- non basta "consegnare un pacchetto" ma bisogna anche installare e configurare il software. Ciò che la licenza GPL ti impedisce, è di rilasciare il tuo software modificato apponendo delle limitazioni alla libertà del software. In pratica, non puoi impedire la copia o la ridistribuzione di versioni modificate, e devi rilasciare il codice sorgente della tua modifica (nel tuo caso, trattandosi di script PHP, la cosa è automatica).
Trovi tutte le risposte ai tuoi dubbi (in italiano) sul sito del progetto Gnu, all'indirizzo http://www.gnu.org/philosophy/free-sw.it.html.

PERCHÉ HAI SCELTO IL TUO NICK?

Sono un assiduo frequentatore del Forum di HJ.it; ho creato un sondaggio che si chiama "Perchè il tuo Nick". Sarebbe bello se poteste pubblicare le risposte dei vari utenti su un numero del Journal di prossima uscita. So che vi arriveranno tante richiesta e magari più sensate della mia, tuttavia è per fare cosa gradita a tutti i frequentatori.

Neuromante

Lo faremo senz'altro in uno dei prossimi numeri. Intanto pubblichiamo il tuo annuncio, in modo che gli altri utenti possano avere il tempo di lasciare il loro messaggio. Il link per arrivare direttamente al thread di discussione si trova nei Contenuti Extra di questo numero.

MODDING GALLERY

Stramitica Redazione di HJ vi ho mandato un paio di immagini del mio pc, con un pò di soft modding il brutto anatroccolo si e presto trasformato....:-) ke ne dite?

KaNeDa

NEWS

NUMERI

38 MILIONI:
Numero dei televisori attualmente presenti in Italia

10-14:
Anni che ci vorranno per sostituire gli attuali televisori con il digitale terrestre

UN MILIONE:
Italiani che si sono aggiunti alla popolazione nazionale del web rispetto allo scorso anno

14 MILIONI:
Stima degli Italiani su Internet

45 MILIONI:
Americani che hanno affollato i siti per cuori solitari nei primi sei mesi del 2003

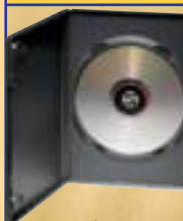
200 MILIONI:
Dollari raccolti dal giro d'affari dei siti americani dedicati ai cuori solitari

350.000:
Canzoni scaricabili da iTunes, l'emporio digitale targato Apple

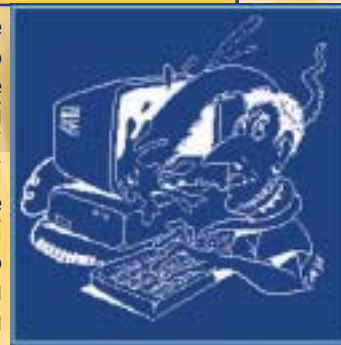
99:
Centesimi di dollaro necessari per scaricare una canzone da iTunes

30 MILIRDI:
Euro persi nel 2002 da Nokia

675 MILIONI:
Euro spesi nel 2001 dalla Pubblica Amministrazione per l'acquisto di software

DVD USA E GETTA

DVD a tempo per Disney. L'azienda ha infatti deciso di servirsi della tecnologia ideata da FlexPlay Technology, che rende praticamente inutilizzabili i supporti dopo due giorni da quando vengono tolti dall'involucro. A contatto con l'ossigeno presente nell'aria, la superficie si deteriora gradualmente, fino al momento in cui diventa completamente nera e il laser dei lettori non riesce più a penetrarla. Lo scopo di Disney con l'adozione di questa tecnologia è di creare veri e propri DVD usa e getta da acquistare al supermercato, in edicola o all'autogrill, vendendoli a un prezzo pari a un noleggio di 48 ore di un normale DVD. L'espediente non creerà particolari problemi ai pirati digitali, che potranno tranquillamente copiare i DVD a tempo esattamente come quelli normali.

BASTA ADDEBITI INDEBITI

Telecom Italia sta dimostrando di voler finalmente fare qualcosa contro i dialer, che stanno diventando un problema sempre più sentito. Prima l'azienda ha deciso di disabilitare gratuitamente le chiamate verso i numeri 709. Adesso ha acconsentito a non far pagare agli utenti gli addebiti in bolletta legati a connessioni con i numeri 709. Tutto grazie a Intesa Consumatori (www.intesaconsumatori.it), che fornisce anche le indicazioni di ciò che bisogna fare per evitare di pagare quando si è stati indebitamente truffati. Anche gli utenti che hanno già pagato la somma da contestare potranno avere il rimborso da parte della società.

SIAMO TUTTI E-MAIL-DIPENDENTI

I responsabili dei sistemi informativi delle aziende sono stressati dai malfunzionamenti della posta elettronica. È quanto emerge da uno studio condotto a livello europeo e americano per conto di Veritas Software. La colpa è degli utenti: davanti a un blocco del sistema un quinto di loro diventa irascibile immediatamente, un terzo nell'arco di cinque minuti e un altro terzo in mezz'ora. Entro una sola ora, l'82% degli utenti sarà veramente incazzato. Un piccolo incidente d'auto, un trasloco o addirittura un matrimonio sarebbero, secondo il 34% del campione considerato, più augurabili di una settimana senza e-mail. Gli italiani sono fra i più irritabili: un solo minuto di blocco fa andare su tutte le furie il 30%, mentre ci vuole più di un'ora per rendere nervoso il 64%. I più irascibili? I responsabili dei sistemi informativi (30%) e i grandi capi (19%).

NEWS

ROBOT, AMORE MIO

Si chiama Linda Lovelace ma non ha niente a che fare con la nota pornostar. È la conseguenza di uno strano fenomeno che si sta diffondendo negli Stati Uniti e in Europa: dare un nome agli elettrodomestici intelligenti. Non si tratta, però, di cagnolini-robot come quelli profetizzati da Asimov in uno dei suoi racconti, ma di veri e propri aspirapolvere che non hanno nulla di somigliante al regno umano o animale. E ciò rende il fenomeno, che prende il nome di "sindrome da robot domestico", ancora più inquietante. Non c'è da stupirsi del fatto che il Paese da cui tutto questo è partito siano gli Stati Uniti, e ancor meno della nascita su Internet di veri e propri gruppi di discussione fra proprietari di questi elettrodomestici, il cui problema principale sembra essere quale sesso assegnare ai loro fedelissimi compagni. Segno dei tempi: la causa principale di questa "malattia" dilagante sembra essere la mancanza di elementi umani, soprattutto fra bambini e anziani, che riverserebbero il loro affetto su queste macchine, capaci di dare loro supporto anche fisico quando la presenza dell'uomo non è possibile.

MICROSOFT VUOLE MANGIARSI GOOGLE

Un nuovo concorrente si affaccia all'orizzonte per Google. Si tratta di Microsoft e, a giudicare dalla prepotenza con cui ha invaso altri settori di mercato che non erano di sua competenza, c'è poco da stare allegri per uno dei più diffusi motori di ricerca presenti sul Web. MSNBot è lo strumento con cui l'azienda ha deciso di tentare l'assalto. Si tratta di un software che, destinato alla indicizzazione dei siti Web, anticipa la creazione del vero e proprio motore di ricerca che i tecnici Microsoft stanno studiando da più di un anno. Fino a questo momento l'azienda si era affidata a Inktomi e Overture, di proprietà di Yahoo!, per le ricerche di MSN. Ora l'azienda ha espresso la volontà di affidarsi, in futuro, a tecnologie fatte in casa.

CASCO PER MOTO PARLANTE

Andare in moto e parlare al telefono. Un'operazione non facile, fino a questo momento. LansLogica ha risolto il problema, creando una soluzione per casco da motociclista basata sulla tecnologia Bluetooth con cui è possibile comunicare con qualunque cellulare dotato di Bluetooth e fra due persone nello spazio di qualche metro. Lo scambio di informazioni avviene agevolmente e in piena sicurezza senza toccare il telefonino. Inoltre è possibile interrompere automaticamente la conversazione tra i due caschi per rispondere a telefonate in arrivo e poi riprenderla. Il processore è all'avanguardia per quel che riguarda il consumo: può infatti funzionare per un'intera giornata con un consumo estremamente ridotto.

HOT!

DVD-VIDEOCASSETTA: 1-0

Già verso la fine del 2001 le povere videocassette non se la passavano certo molto bene, surclassate dai nuovi veri strumenti di riproduzione del futuro: i DVD. A quei tempi per la prima volta negli Stati Uniti le vendite dei DVD avevano superato quelle delle videocassette. Ma, non contenti di aver vinto una battaglia, i nuovi supporti hanno voluto vincere tutta la guerra e si sono fatti avanti a spron battuto anche nell'ambito del noleggio, in cui la videocassetta deteneva ancora un seppur pallido primato. Quest'ultima, amara sconfitta, fa di lei uno strumento sorpassato e messo da parte per eventuali futuri musei di modernariato.

IL WI-FI PARTE DALLE UNIVERSITÀ

Spetta all'Olanda il primato nella sperimentazione del wi-fi. Grazie alla collaborazione di Cisco e IBM, infatti, è stato possibile realizzare all'università di Twente, in Olanda, 650 hot spot che permetteranno agli studenti di collegarsi ovunque senza fili. Sarà sufficiente possedere un computer portatile o un palmare, e il gioco è fatto, in quattro e quattr'otto chiunque potrà ritrovarsi collegato a internet in qualunque parte dell'università si trovi. L'ateneo olandese può così vantarsi del fatto di essere stato il primo a connessione totale, nonché la più grande rete wi-fi, in Europa.

NEWS

SITI WEB

MATRIX ALLA TEDESCA

www.matrix-xp.com

Se volete consolarvi dalla delusione del secondo episodio di Matrix, certo non all'altezza del primo, ecco un sito che fa per voi: vi troverete un esilarante remake del film (molto più corto, non vi preoccupate) fatto da alcuni ragazzi tedeschi, con finale a sorpresa in cui non poteva mancare lo sbeffeggio a Microsoft. Tutto da vedere…

HELLO KITTY SPLATTER

www.happytreefriends.com/watch_episodes

Apparentemente sembra un sito per adolescenti romantiche, tutto colori pastello e personaggi degni di essere compagni di gioco di Hello Kitty. Non lasciamoci ingannare dalle apparenze, però: collegandoci a questo sito troveremo una serie di filmati splatter a confronto dei quali South Park sembra robetta da bambini.

ABANDONWARE

www.sitosenzanome.it

Lo scopo del SitoSenzaNome.it è quello di far conoscere ai più giovani e riavvicinare i più vecchi al fantastico mondo dei giochi d'epoca, vere colonne portanti del mondo videoludico odierno. Tutti conoscono Quake 3, Red Alert o FIFA 200x. Ma quanti di voi conoscono i loro illustri predecessori: Wolfenstein 3D, Dune 2 e FIFA International Soccer? Tra questi cimeli si annida anche qualche sparuto titolo per Windows ma quella che l'autore del sito vuole esaltare sulle sue pagine è l'éra del gioco per il mitico MS-DOS, a partire dal tempo pionieristico delle avventure testuali. Sul sito anche l'unico, vero e originale Manifesto del Movimento Abandonware.

KAZAA CERCA UN DIALOGO CON LE CASE DISCOGRAFICHE

Dopo Napster, adesso è la volta di Kazaa, attualmente il più popolare fra i siti che permettono di scaricare e scambiare musica su Internet gratuitamente, di rinnegare le proprie origini per vendersi al miglior acquirente. La responsabile Kinni Hemming ha infatti avanzato una proposta di dialogo con le grandi case discografiche e gli studi cinematografici di Hollywood, proponendosi come veicolo indispensabile per la commercializzazione dei loro prodotti in territori oggi dominati dalla pirateria. Lo scopo di Hemming non è certo di diffondere il modella peer-to-peer gratuito, come lo è stato fino a questo momento. Vorrebbe infatti trasformare Kazaa nel più importante strumento di diffusione a pagamento della musica prodotta dalle stesse etichette discografiche. Secondo Hemming, le tecnologie peer-to-peer si sono ormai affermate fra il pubblico e le case discografiche non devono far altro che prendere atto di questo e comportarsi di conseguenza. Per il momento, la sua proposta di trattativa non ha ricevuto alcuna risposta.

TUTTI A CACCIA DI ZERBINI

Non si può certo dire che gli americani non siano un popolo originale! E lo dimostra l'ultima iniziativa che ha come centro propulsore, ancora una volta, il web. O meglio, l'e-mail. Si chiama "Mob Project" ma in realtà è una non-progetto, ovvero, non ha alcuna finalità specifica. Se non riunire in un determinato punto della città (in questo caso si tratta di New York) una folla di persone (mob, per l'appunto) con un compito decisamente fuori dal comune: nell'ultimo caso, per esempio, recarsi alle ore 17.00 al reparto tappeti dei grandi magazzini Macy's, al terzo piano, per chiedere tutti quanti informazioni sullo stesso tipo di zerbino. Il famigerato ideatore di tutta questa messinscena è un certo Bill – di lui si conosce soltanto questo soprannome – che è riuscito a radunare 250 persone meticolosamente dedite allo scopo. Il tutto organizzato, appunto, tramite e-mail, senza alcuna web page come punto di coordinamento, ma contando soltanto sul passaparola. Unico vincolo: la convocazione deve essere finalizzata soltanto ad atti insensati.

IL POPOLO INTERNET TEME PER LA PROPRIA IDENTITÀ

Secondo quanto emerge da un'indagine commissionata da RSA Security, la paura più grande per chi naviga su Internet è che qualcuno possa sottrarre a ognuno la propria identità utilizzandola per scopi illeciti. Malgrado questo, oltre il 40% dei consumatori non ha ancora implementato alcuna forma di protezione contro gli attacchi che minacciano la sicurezza. Fra coloro che hanno invece implementato misure di sicurezza, il 39% ha installato un software antivirus. La paura di essere derubati della propria identità non è comunque sufficiente a far cambiare al 42% degli intervistati le proprie abitudini di acquisto.

NEWS

UN SOFTWARE CONTRO IL GERGO PROFESSIONALE

Basta ai fastidiosissimi termini professionali dedicati agli "addetti ai lavori". Arriva Bullfighter, il software creato per eliminare da ogni forma di comunicazione d'affari tutte le espressioni professionali. Già il nome è tutto un programma. La traduzione letterale è "torero", ma in realtà è la metafora di chi combatte le fregnacce. In questo caso, tutte quelle espressioni da noi e dai nostri lettori tanto odiate quali "sinergie", "paradigma", e chi più ne ha più ne metta. Pare che queste fregnacce, definite "bullwords", siano all'incirca 10mila, anche se il povero Bullfighter, scaricabile gratuitamente all'indirizzo Internet www.dc.com/bullfighter, è stato programmato per eliminarne automaticamente soltanto 350. Chissà come se la cava con termini come w4r3z o 1337.

ARRIVA IL WEB SEMANTICO

Motori di ricerca più rapidi e risultati più precisi. Questo lo scopo del Web semantico, promosso dal consorzio W3C (World Wide Web Consortium), da varie aziende informatiche e dal mondo accademico. Per fare ciò è necessario rinnovare tutta l'infrastruttura Web per favorire una ricerca più rapida delle informazioni. Al centro di questo nuovo sistema ci sono i database con le loro modalità di pubblicazione, conservazione e gestione dei dati per la loro visualizzazione sul web. Dal punto di vista del navigatore, tutto ruota quindi attorno ai motori di ricerca e ai risultati che si ottengono a seguito di una interrogazione. Ad oggi la rete fornisce risultati per nulla soddisfacenti, soprattutto al primo tentativo. Quasi un paradosso, se si pensa al numero impressionante di informazioni presenti su Internet. A quanto pare, però, è difficile reperirle. Il web semantico propone la creazione di un sistema intelligente in grado di interpretare i contenuti. Per fare questo l'HTML non basta più ed è quindi necessaria la migrazione verso l'XML, un linguaggio che offre maggiori possibilità di personalizzazione rendendo i risultati di ricerca molto vicini a quelli desiderati.

IL TELEFONO CHE LEGGE LE LABBRA

Tecnologia al servizio dell'umanità. Spesso abbiamo qualche difficoltà a dare un significato concreto a questo slogan ormai stra-abusato. Non in questo caso, però, in cui i risultati concreti e l'utilità dello strumento sono più che evidenti. Stiamo parlando di Synface, che sta per "volto sintetico", un telefono visuale per audiolesi dotato di un software che consente di riprodurre i movimenti del volto su un display collegato all'apparecchio. La faccia "digitale" creata dal computer in tre dimensioni è in grado di cambiare espressione, aggiungendo preziose informazioni per la corretta interpretazione della frase pronunciata. I primi prototipi funzionanti sono attesi per i prossimi due o tre mesi, in modo che la sperimentazione possa avere inizio in autunno nel Regno Unito.

I VIDEOGAME VANNO IN TELEVISIONE

Si chiama G4 ed è il primo canale televisivo via cavo interamente dedicato al mondo dei videogame. E se questo non stupisce, dato il clamoroso sviluppo che ha avuto negli ultimi anni l'industria dei videogiochi, quello che stupisce sono i risultati di pubblico ottenuti. Creato un anno fa da Comcast con un budget modesto (150 milioni di dollari) che dimostra quanto poco l'azienda credesse nel successo dell'iniziativa, la Cenerentola in questione ha invece prodotto risultati sbalorditivi, portando al colosso delle TV via cavo una media di quasi un milione di spettatori, quasi il doppio dell'obiettivo programmato. Uno dei programmi di maggiore successo è Pulse, dedicato ai trucchi che permettono di eludere le regole del gioco.

ARROTONDARE LO STIPENDIO

Chi lavora in Microsoft guadagna bene, si sa. Soprattutto se decide di arrotondare lo stipendio con una buona dose di iniziativa e spirito imprenditoriale, come ha fatto un tale Richard Gregg. Questo dipendente, sfruttando la sua posizione nell'azienda, acquistava grossi quantitativi di software a prezzi vantaggiosi che poi rivendeva all'esterno. Il business gli è fruttato nell'ordine: 17 milioni di dollari, il licenziamento in tronco e un procedimento legale. Complimenti Richard!

PIRATERIA:

Studi statistici e pirateria del software: un punto di vista differente.

Da qualche settimana, la BSA (Business Software Alliance), organizzazione senza fine di lucro che tutela gli interessi delle maggiori società operanti nel settore informatico (tra le quali Microsoft, Autodesk, Sony ed Apple, solo per citarne alcune), ha reso noti i risultati di uno studio commissionato alla società IDC. In base a questo studio, **la diminuzione della pirateria informatica consentirebbe la crescita del settore IT e la creazione di migliaia di nuovi posti di lavoro**.

Secondo gli esperti della IDC, il settore IT potrebbe beneficiare della riduzione della pirateria informatica fino a crescere del 50% in più rispetto alle aspettative, fornendo fino a 1.500.000 di nuovi posti di lavoro.

L'incremento del gettito fiscale è stimato in 57 miliardi di euro, mentre la crescita economica complessiva dei paesi interessati dal fenomeno potrebbe raggiungere i 357 miliardi di euro.

Risultati decisamente interessanti, che dovrebbero far felici i capi di stato che hanno promesso migliaia di posti di lavoro per i prossimi anni e che, indubbiamente, lasciano intravedere un roseo futuro per tutti i giovani in cerca di occupazione.

>> Promesse da marinaio?

Peccato che, alle cifre ragguardevoli e precise fornite nella prima parte dello studio, facciano seguito molti verbi al condizionale e molte affermazioni generiche in merito ai benefici dei quali avrebbero già goduto i paesi che da tempo sono in prima linea nella lotta alla pirateria informatica.

Secondo altre fonti, altrettanto autorevoli, **l'industria IT degli Stati Uniti è talmente in crisi da minacciare l'esistenza stessa della Silicon Valley**, così come in Europa qualsiasi mercato, non solo quello tecnologico, si trova ad affrontare **una recessione senza precedenti**. La recessione è aggravata dalle ripercussioni della moneta unica europea sui mercati mondiali, che frena pesantemente le esportazioni, rendendo economicamente più conveniente acquistare in altri paesi extraeuropei.

Il mercato del lavoro, infine, accusa sempre più il divario tra preparazione scolastica ed esigenze aziendali. In sostanza, gli studenti di oggi non apprendono ciò che servirà loro nelle aziende di domani (soprattutto perché le scuole non sembrano in grado, nel breve periodo, di aggiornare i programmi didattici all'evoluzione tecnologica), e ciò introduce ulteriori difficoltà per l'inserimento nel mondo del lavoro, che si traduce in ulteriori posti di lavoro persi (e non guadagnati) a causa dell'IT.

>> Vediamoci chiaro

Il personal computer è nato per migliorare la produttività individuale. Ciò significa che, rispetto al passato, dovremmo lavorare meno e meglio, perché il computer consente di fare in un'ora ciò che prima impegnava un lavoratore per tre ore.

Quindi, se la matematica non è un'opi-

NEWBIE

i conti non tornano

nione, oggi, **su un'ipotetica giornata di nove ore di lavoro, ogni lavoratore dovrebbe avere sei ore libere**.
Questo vantaggio, tuttavia, nel mondo "accelerato" in cui viviamo, è stato sfruttato per incrementare i profitti; il che significa che oggi un impiegato lavora ugualmente nove ore, ma produce (e si stressa) il triplo di prima. Problemi d'analisi psichiatrica a parte (la malattia più diffusa nei paesi civilizzati è la depressione), ciò determina **una riduzione del personale pari a due terzi**. Il che significa che, sempre a causa dell'evoluzione tecnologica, a parità di produttività si perderebbero i due terzi dei posti di lavoro prima disponibili. In realtà, per fortuna, le cose non stanno così, e semplicemente si produce di più per generare più profitti.
È interessante, infine, verificare che a promuovere leggi sempre più repressive contro la pirateria informatica - preoccupandosi di spingere i governi ad adottarle, finanziando e pubblicando studi come quello qui commentato - sono le stesse aziende che, grazie ad essa, **hanno affermato la propria presenza monopolistica nel settore di riferimento**.

>> A chi giova?

Autocad è il programma di disegno tecnico più usato al mondo.
Windows e **Office** sono il sistema operativo e la suite da ufficio più diffusi al mondo.
La **Playstation** è stata la consolle da gioco più venduta al mondo.
Sarà un caso che nelle facoltà di architettura ed ingegneria gli esami si sostengano su Autocad, nonostante sia abbastanza evidente che gli allievi, salvo qualche eccezione, **non potendosi permettere il lusso di spendere circa 5000 euro** per acquistare una copia ufficiale del programma, **ricorreranno ad una copia pirata?**
Sarà un caso che nelle scuole di ogni ordine e grado e negli uffici pubblici, negli anni '90 (cioè quando Windows e Office non erano uno standard e dovevano fare i conti con altre realtà ben più affermate, come Wordstar, Lotus 123, dbase III, Unix, Xenix eccetera), **il pacchetto Office e il sistema operativo Windows si siano diffusi grazie alle copie pirata stranamente disponibili in quantità industriali** - costringendo gli utenti e le aziende a dotarsi dei medesimi programmi, per ragioni di compatibilità ed interoperabilità - e che, negli stessi anni, nonostante il fenomeno fosse ben più radicato di oggi, l'attività antipirateria di molte aziende era praticamente inesistente?
Sarà un caso che la Playstation abbia sbaragliato i propri concorrenti perché **i giochi su CD potevano essere facilmente copiati**, e a prezzi irrisori, e quelli dei concorrenti no?
In conclusione, sorge legittimo il sospetto che, per le aziende del settore, la pirateria informatica sia stata **un fenomeno da supportare** (più o meno ufficialmente) negli anni 90, quando il mercato stava selezionando gli operatori che avrebbero dovuto dettare gli standard negli anni successivi, e sia diventato un **fenomeno da arginare** solo da qualche anno, cioè **da quando le poche aziende sopravvissute sono in grado di controllare un mercato in cui gli utenti sono ostaggio dei dieci anni di formazione professionale e codificazione dei dati**.
Con buona pace delle autorità Antitrust, che sembrano ignorare lo stato di dipendenza psicologica e tecnologica degli utenti dalle major del software, della musica e del cinema.
Quanti utenti, infatti, non migrano a Linux - nonostante i numerosi vantaggi, anche di ordine economico - per la difficoltà di imparare a utilizzare un nuovo sistema operativo? E quante aziende non possono migrare al free software per la difficoltà di riconvertire procedure e archivi studiati e codificati per decenni per il mondo Windows, e per i costi connessi alla riqualificazione del personale?
Dal punto di vista giuridico, infine, **è quantomeno discutibile che gli interessi commerciali delle aziende debbano essere tutelati dalle Forze dell'Ordine** e dalla Magistratura, che sono pagati con i soldi dei cittadini.
La licenza d'uso del software è paragonabile al canone di locazione di un appartamento; **ma per liberare un appartamento da un inquilino moroso o abusivo non è possibile ricorrere alle Forze dell'Ordine senza aver preliminarmente aperto un'azione civile per sfratto.**

Gianluca Pomante

STORIA ED ETICA HACKER

Chi sono, cosa fanno e in cosa credono i veri hackers

Gli hacker sono sempre esistiti… Sono gli onnivori della conoscenza… gli eroi della rivoluzione informatica… i ricercatori assidui della perfezione estrema… i pionieri delle nuove frontiere tecnologiche.

Smanettano nei meandri della Rete, agendo in simbiosi con i calcolatori, fanno parte di una comunità underground che non ha mai avuto il rispetto che si merita. Sono i "dietro le quinte" del mondo dell'Information Technology, il motore del progresso.

Vengono disegnati dai mass media quali criminali, terroristi informatici, pirati virtuali. Esplorano… e li chiamate criminali. Cercano la conoscenza… e li chiamate criminali. Esistono senza colore della pelle, senza nazionalità, senza pregiudizi religiosi… e li chiamate criminali. Hanno progettato, costruito e sviluppato la Rete… e li chiamate criminali. Hanno creato un OS stabile e sicuro, personalizzabile e open source… e li chiamate criminali.

Sì, è vero. Sono dei criminali. **Il loro crimine è la curiosità. Il loro crimine è quello di giudicare le persone in base a quello che pensano e dicono, non per come appaiono. Il loro crimine è quello di dimostrare al mondo le vulnerabilità del vostro software. Il loro crimine è quello di saperne più di voi, di essere più furbi di voi, di essere più intelligenti di voi… reati che non potrete mai perdonare.**

Non li temete dunque; perché non c'e' niente di nascosto che non debba essere scoperto, ne' di occulto che non debba essere rivelato.

>> Un'idea sbagliata

I mass media hanno diffuso da sempre un' idea distorta della figura dell'Hacker. Nell'attuale mondo tecnologico dove Internet sta assumendo maggiore importanza rispetto ai mass media, **l'Hacker viene visto come la parte "cattiva" del Web**.

Il comune lettore/utente è abituato a pensare all'Hacker quale un ragazzo, al lavoro, al buio, chino sul computer, circondato da apparecchi tecnologici, da scarti di pizza, da tazze sporche di caffè, mozziconi di sigaretta e con ogni superficie piana occupata da manuali, documentazione e stampate di vario genere, intento a digitare comandi e a lanciare attacchi verso un bersaglio posto all'altro capo del mondo. È così fossilizzato su questa idea che non riesce neanche a immaginare che possa essere sbagliata.

Questo perché **pur di rimediare uno straccio di notizia sensazionalistica, l'Hacker viene catapultato nei titoloni dei giornali** e usato come unico capro espiatorio. Ciò è causato da una scarsa preparazione in materia da parte del giornalista, ma anche da un forzato adeguarsi di chi scrive a una presunta ignoranza del comune lettore.

Ma la figura dell'Hacker vista come un asso dell'informatica, capace di entrare in un qualsiasi sistema informatico, **catalizza l'interesse, soprattutto degli adolescenti, verso questo mondo**. E se state leggendo questa rivista, probabil-

mente vuol dire che anche voi siete rimasti affascinati dal "sentito dire" dell'Hacker.
Eppure le responsabilità **non sono da attribuire esclusivamente a Tv e giornali**. Infatti surfando nella Rete in siti dedicati (per così dire) al mondo dell'hacking, incontreremo documenti che trattano il termine "Hacker" parlando di **mail bombing, password cracking e altre lamerate del genere**. I WebMaster di questi siti sono ragazzini che sperano di guadagnare fama nel mondo dell'hacking e fanno di tutto per pubblicizzare il proprio sito (iscrizione alle TOP 100, spam nei forum eccetera). Nella maggior parte dei casi questi siti si presentano come "grandi portali underground" e in realtà sono solo una grande raccolta di manuali e articoli raccolti nella Rete, scritti da persone che raccontano ciò che mangiano e ascoltano; molto spesso nascondono dialer o trojan e non trattano argomenti quali etica e cultura hacker, o se questi vengono trattati sono sempre copia & incolla presi dalla Rete e che discordano con il resto del sito.

Tutto ciò contribuisce ancor più a diffondere l'idea di hacker quale criminale.
A peggiorare la situazione ci sono molteplici persone che girano nelle chat e soprattutto in IRC, vantandosi di essere hacker e credendosi tali solo per il fatto di essere riusciti a usare un trojan, o per il loro primo defaced.
In linea di massima quindi le prime cose da evitare sono quello di leggere articoli informatici scritti dai quotidiani nazionali. Se volete tenervi sempre informati sulle ultime notizie dell'IT, iscrivetevi a qualche buona newsletter. Le migliori sono quelle di Punto Informatico (www.punto-informatico.it), di Programmazione.it (www.programmazione.it), di Zeus News (www.zeusnews.it) e di Porta Zero (www.portazero.info).
Inoltre non frequentate siti che trattano in maniera indecente l'-hacking e **iniziate a visitare siti seri che trattano questo argomento nella maniera più etica possibile** (trovate una lista di link nei Contenuti Extra).
Per quanto riguarda invece IRC e chat, il consiglio è quello di non frequentarli e preferire i forum a quest'ultimi (ad iniziare dal forum di HJ) se avete intenzione di chiedere o condividere informazioni.

>> La definizione

Iniziamo a fare ordine e cerchiamo di dare una definizione di hacker.
Non esiste in realtà una definizione unanime di hacker: ce ne sono molte e darne una completa è compito assai arduo. La definizione ufficiale la trovate allo Jargon File, il più prestigioso dizionario hacker.
Possiamo qui affermare che il vero hacker **è l'esperto di sicurezza informatica che si diletta nell'esplorazione dei dettagli di tutti i sistemi di programmazione, nell'espansione delle loro capacità oltre i limiti**. È colui che prova piacere nella risoluzione dei problemi e che crede ciecamente nei principi dell'open source. Egli non defaccia mai un sito, e non è geloso delle sue conoscenze. Anzi, cerca di condividerle con altri, facendo sempre attenzione a non divulgarle a gente inaffidabile. È colui che studia e ristudia e cerca di imparare sempre dai propri errori; si scrive da sé i programmi e utilizza altri software perché ritiene che chi li ha creati sia più bravo di lui. Esercita l'autocritica. È colui che non usa software proprietario e che cerca sempre di essere un autodidatta. hacker è colui che non si definisce tale, lasciando che gli altri lo facciano per lui. È colui che non entra nei sistemi per far danni ma solo per segnalarne la falla e la risoluzione all'Admin. È colui che si tiene costantemente aggiornato e non smette mai di imparare. L'Hacker sa solo **di non sapere**.
Questo definizione è relativa ad un ambito informatico. Ma **l'-hacking deve essere inteso come stile di vita**, un modo di essere, quasi una concezione filosofica esistenziale, non solo come qualcosa di strettamente tecnico. Essere "Hacker dentro" è come essere innamorati: è innanzitutto un'emozione. Innamorati della propria scienza o del proprio interesse primario, a prescindere dalle conoscenze tecniche. Sarà poi questo innamoramento che culminerà in una conoscenza completa, in approfondimenti, sviluppi e divulgazione d'informazione dando vita all'Hacker dentro e fuori. Ed è per questo che non si è hacker solo d'informatica. Si può essere hacker in un qualsiasi campo della scienza.

>> I valori

Vediamo quali dovrebbero essere i valori dell'Hacker.

1. L'accesso ai computer deve essere assolutamente illimitato e completo

L'Etica hacker si basa sul concetto che qualsiasi software o hardware deve poter essere "smontato", analizzato, studiato, approfondito e migliorato fino al raggiungimento della perfezione (che non potrà mai esistere come tale, perché per ogni traguardo raggiunto se ne prospetterà un altro ancor più allettante).
Tutto ciò che non permette questo lavoro o lo ostacola (leggi, aziende, persone, barriere fisiche, software e hardware) sarà sempre criticato e odiato dagli hackers. Ecco perché esiste un atteggiamento di diffuso disprezzo verso il software proprietario.

2. La diffusione e condivisione delle informazioni deve essere libera

Uno dei principi dell'Hacking è la condivisione e la diffusione di informazioni. Mentre un tempo reperire materiale era difficile, oggi invece la sua disponibilità sulla Rete ha diffuso la conoscenza. In ambito informatico, questo è ulteriormente utile perché consente di progredire più in fretta ed evitare che un qualcosa di già realizzato debba essere ripetuto. Anche in questo caso, gli hacker odiano tutto ciò che impedisce la libera circolazione di dati, ed è per questo che odiano la normativa EUCD. Inoltre la diffusione della conoscenza deve essere esercitata in particolare dagli hackers che hanno il dovere di istruire chi ne sa meno di loro.

3. Le persone devono essere giudicate dall'operato.

Tutti devono essere giudicati in base a quello che scrivono e fanno. Non devono influire fattori come l'età, la razza, il sesso, il colore della pelle o il ceto sociale o i diplomi e le lauree. Giudicare qualcuno in base a questi parametri ha un sapore chiaramente razzista e denota una enorme superficialità e incapacità di giudizio.

4. La passione genera il progresso

La "legge di Linus Torvals" insegna che sono tre le motivazioni essenziali di un individuo che costituiscono le spinte direttrici del progresso: sopravvivenza, legami sociali e intrattenimento. Assistiamo invece da parte dell'Hacker ad un uso del computer che non si colloca solo nello stadio di mera sopravvivenza o va ad infittire la rete di rapporti interpersonali. Il computer non è solo uno strumento di lavoro o del tempo libero ma assume una centralità nell'esistenza dell'Hacker per il quale diventa un serio impegno, permanente e ricco di passione e di spirito creativo. Ecco perché il vero hacker fatica a distinguere dove comincia il lavoro e termina il divertimento e viceversa.

5. Internet è nata per essere libera.

La Rete è nata per la condivisione libera e gratuita di materiale e informazioni, annullando le distanze territoriali. Ma, come in tutto ciò che è una possibile fonte di guadagno, anche Internet sta subendo (e in gran parte ha già subito) un processo di monopolizzazione. E ce ne accorgiamo navigando o scaricando la posta. Ormai tutto è lecito per indurti a entrare in un sito, i dialer si installano automaticamente e non comunicano il costo della connessione, si aprono 13 pop-up all'apertura di un sito, gli indirizzi e-mail vengono venduti ai maggiori offerenti spammer, i cookie s'impadroniscono di informazioni non dovute. L'Hacker ha il dovere di contestare e combattere questa politica.

6. La tutela della privacy

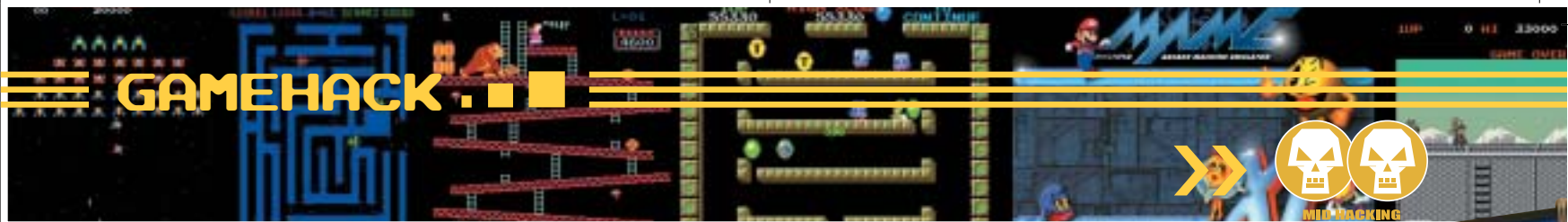
La privacy dell'utente deve essere rispettata. Allo stato attuale delle cose viene sistematicamente violata tramite progetti, ad esempio, quali Echelon. E, dopo gli eventi legati all'11 settembre, la privacy è diventata la vittima sacrificale sull'altare della lotta al terrorismo. Essere hacker vuol dire anche acquisire questa consapevolezza e contribuire a diffonderla, cercando magari di garantirsi una pur minima tutela con strumenti di crittografia.

7. Un sistema insicuro è un sistema a rischio

Qualsiasi sistema informatico che presenti falle di sicurezza è un sistema suscettibile di attacchi da parte di malintenzionati. L'Hacker è fermamente convinto che, una volta analizzato il bug, sarà necessario comunicarlo all'Admin in questione, magari fornendogli anche la risoluzione. Tutto ciò senza provocare alcun danno.

Leonardo Vaghaye 'Milo Cutty'
milo.cutty@libero.it

Questo articolo è liberamente ispirato a documenti e libri scritti da personaggi protagonisti sulla scena internazione del mondo dell'hacking, quali Eric S. Raymond, Steven Levy, Pekka Himanen e The Mentor, e a alcuni post su cui si è discusso sullo stesso forum di Hj. Lo scopo dell'articolo è educare all'Etica hacker e chiarire il vero significato del termine "Hacker".

MID HACKING

MAMECAB: FATTI UN GIOCO DA SALA

Vi siete appassionati a Mame, ma giocare su un PC non ha lo stesso fascino dei giochi da sala? Costruitevi un cabinet!

Se dopo aver usato Mame in versione Dos o Windows (o Linux, o Mac, Amiga…) vi è venuta voglia di far rinascere un cabinet da sala giochi, avete qualche speranza di riuscire a farlo. La strada non è impossibile da percorrere, ma dipende dal grado di fedeltà che vorrete dare alla vostra sala giochi da casa. Per quanto riguarda le sale giochi, il periodo migliore è stato certamente quello a metà degli anni '80, per cui la nostra missione sarà quella di riprodurre il nostro cabinet proprio a imitazione di quell'epoca. Per il resto si tratta solo di munirsi di un po' di pazienza e di fortuna.

>> Procurarsi il materiale

Ovviamente bisogna partire dal reperimento di un cabinato originale. Per trovarlo, io ho personalmente iniziato l'indagine dalla sala giochi dove passavo la maggior parte del mio tempo (anziché correre il rischio di farmi interrogare a scuola) per farmi dire da chi prendevano i giochi: i cosiddetti "coin-op" vengono affittati da società specializzate nella sola vendita di videogiochi "da bar". Si tratta in pratica di immensi capannoni, tuttora esistenti, di solito situati in periferia e che contengono un paradiso di cabinati, solitamente buttati lì e ammassati. Al giorno d'oggi i vecchi cabinati sono infatti considerati alla stregua delle vecchie '500: mitiche ma che non interessano più la massa, quindi semplicemente "oggetti" che rubano spazio alle nuove fiammanti macchinette del videopoker! Alcuni li tengono perché riescono a piazzarne ancora in alcuni paesi esteri (soprattutto Africa). Nel caso in cui non abbiate un punto di partenza per questo, basta andare sul sito delle pagine gialle (www.paginegialle.it) e ricercare le aziende sotto la categoria "videogiochi, flippers e biliardini – vendita al dettaglio e noleggio". Dopo qualche telefonata riuscirete sicuramente a trovare il posto giusto nella vostra città.

Il prezzo di un cabinato può variare tra gli 80 e i 120 euro: se vi chiedono di più, cambiate posto, tanto nel momento in cui uscirete dal negozio vi correranno appresso per venirti incontro con un forte sconto: ricordate che per loro sono solo un peso inutile, e che prima o poi se non li smerciano dovranno demolirli.

>> Il cabinato

Assicuratevi che il cabinato sia dotato di monitor e di alimentatore. Prima di portarlo via, verificate che tutto funzioni, facendovi attaccare un gioco qualsiasi, in modo da provare direttamente il vostro cabinato ed essere certi che tutto sia a posto. In particolare, pro-

Il cabinet visto da dietro. A sinistra il PC; se seguite i cavi del video e della tastiera arrivate sulla destra alla schedina J-Pac che interfaccia il connettore Jamma del cabinet al PC.. In basso l'alimentatore del monitor e un subwoofer Creative per dare più profondità al suono

vate i joystick in tutte le direzioni e tutti i pulsanti per evitare fregature. Internamente, tutti i videogames funzionano con la medesima "interfaccia": all'interno dei cabinet non c'è altro che la scheda del gioco collegata ad un connettore uguale per tutti i giochi, e che si chiama JAMMA: per "trasformare" il cabinet in un altro gioco basta sfilare la scheda del vecchio gioco dal connettore JAMMA e infilare la scheda del nuovo gioco sullo stesso connettore. Alcune schede particolari (come alcune edizioni di Street Fighter) prevedevano il "JAMMA+", ovverosia sempre un JAMMA ma con un secondo connettore che consentiva di utilizzare più pulsanti di quanti il JAMMA ne prevedesse (sei, nel caso di Street Fighter).
Se siete in vena di spese, e per avere quel gusto del vero originale, una "jamma-game-board" può essere l'oggetto giusto per i vostri desideri. La scheda di un gioco originale può costare tra i 30 e i 50 euro, ma dopo quella spesa il gioco sarà vostro per sempre, e non sarà più necessario inserire scintillanti monetine, una dopo l'altra. Già che ci si siete, fatevi dare dal noleggiatore anche qualche pulsante in più, e almeno un joystick di scorta, non si sa mai dovesse tornare utile in futuro…
Per i veri cultori, la ricerca del cabinato giusto che abbia i joystick giusti. Quelli "veri" sono quelli a levetta, corti e neri che montano i microswitch della honeywell come quelli prodotti dalla edierre (www.edierre.it) modello "01" (il cui prototipo venne realizzato al tornio artigianalmente nel 1982). Sicuramente non sono i più comodi ed ergonomici, ma avevano il loro fascino particolare e soprattutto sono tuttora indistruttibili, a 20 anni dalla loro creazione... Tornando al cabinato, tenete presente inoltre che vi servirà una buona dose di alcol, detersivo e quant'altro, poiché di solito lo stato interno dei cabinet non è proprio il massimo in quanto a pulizia…
Ma ora torniamo al nostro progetto, che è quello di avere l'intera sala giochi in casa…

>> L'emulatore

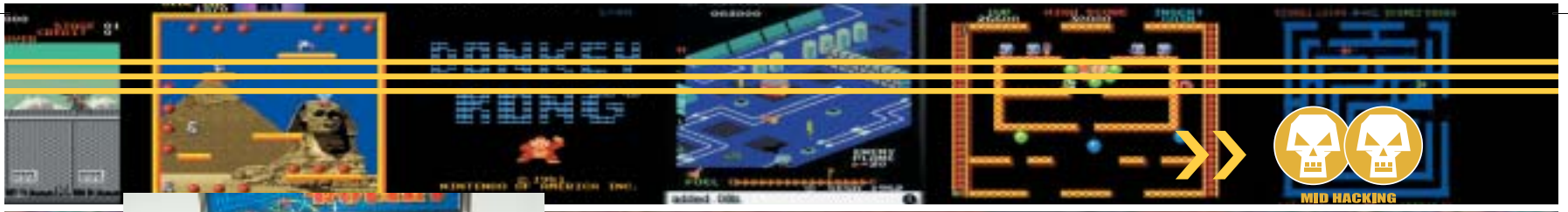
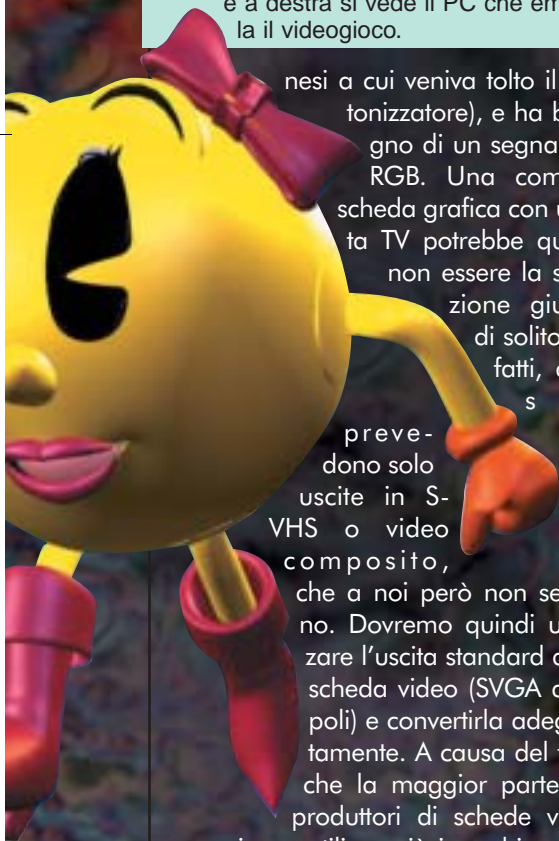
Esistono svariati emulatori "predisposti" per emulare i coin-op nello specifico su dei cabinati: questi devono essere in grado di far uscire il segnale dalla scheda video ad una determinata frequenza, e poiché i vecchi registri VGA vengono oramai ignorati dalla maggioranza delle case produttrici, dovrete andare alla ricerca della giusta scheda grafica (ma di questo ne parleremo in dettaglio più avanti in questo articolo). Come emulatore vi consigliamo caldamente AdvanceMame (http://advancemame.sourceforge.net) che, assieme ad AdvanceMenu (stesso sito) potrà esservi decisamente di aiuto. AdvanceMame è in grado di forzare le schede a uscire con una determinata frequenza (sul sito troverete anche la lista delle schede grafiche testate) ed emula i giochi caricandoli dalle ROM (le stesse che si usano per Mame). AdvanceMenu invece è il programma che gestisce la presentazione della lista dei giochi (sempre forzando l'uscita su monitor arcade), e che potrete utilizzare per scegliere, utilizzando il joystick sul cabinato, il gioco che volete caricare.

>> Il PC

Passiamo ora al PC: non ti servirà una macchina troppo "spinta": basta anche un vecchio PIII-550 per far funzionare decentemente l'80% dei giochi. Come memoria, 64MB possono bastare, 128MB vanno di lusso. Per l'hard disk potete puntare anche a un 9 Gbyte, se però avete lì sul tavolo un 20 Gbyte e non sapete che farci, potete sicuramente starci molto più comodi. Una qualsiasi tastieraccia e un mouse potranno rivelarsi indispensabili soprattutto durante la configurazione.
La parte più impegnativa del progetto sarà in assoluto il video, quindi per sapere qual'è la scheda più adatta allo scopo, dovrete continuare a leggere.

>> Le schede video...

Il problema è che all'interno della maggior parte dei coin-op c'è un monitor NTSC che funziona, come già accennato, a delle frequenze particolari (15 Khz). Quello schermo è praticamente uguale a un televisore (di solito erano proprio comuni televisori americani o giappo-

La scheda J-Pac della Ultimarc (www.ultimarc.com) permette di fare funzionare tutto senza grande fatica. In alto si collega il connettore Jamma del cabinet, e in basso il cavo tastiera del PC e la scheda video. J-Pac taglia automaticamente la frequenza della Vga, evitando di danneggiare il monitor del cabinet. Notate a sinistra altri connettori per pulsanti addizionali, visto che il Jamma supporta solo tre pulsanti di fuoco per ogni giocatore, mentre alcuni giochi ne richiedono fino a otto (ma dopo che ne avete installati quattro sono più che sufficienti).

La scheda originale di Street Fighter 2; i chip in alto a sinistra con l'etichetta bianca sono le Eprom con il programma. In basso a sinistra la gettoniera funzionante (monete da 200 lire) e a destra si vede il PC che emula il videogioco.

nesi a cui veniva tolto il sintonizzatore), e ha bisogno di un segnale in RGB. Una comune scheda grafica con uscita TV potrebbe quindi non essere la soluzione giusta: di solito, infatti, queste prevedono solo uscite in S-VHS o video composito, che a noi però non servono. Dovremo quindi utilizzare l'uscita standard della scheda video (SVGA a 15 poli) e convertirla adeguatamente. A causa del fatto che la maggior parte dei produttori di schede video oramai non utilizza più i vecchi registri VGA (con l'eccezione della stragrande maggioranza dei modelli ATI), bisognerà riuscire a procurarsi una scheda (l'ATI Rage 128 può andare benissimo) che sia prevista dall'emulatore, e cominciare a effettuare delle prove. Il tutto comunque dopo aver convertito il segnale... Vedremo però che per questo problema e per il prossimo esiste un'unica soluzione.

>> ...e il resto

Altro problema che avrete sarà quello di dover collegare il joystick, i pulsanti dei giocatori e la "gettoniera" (dove si inserivano i "gettoni") alla tastiera (Mame è un programma per PC, e in quanto tale si aspetta di ricevere input da tastiera, e non da strana ferraglia). Sembra un controsenso, ma dovremo emulare la pressione dei tasti della tastiera (che a loro volta emulano i pulsanti del cabinet...) utilizzando i pulsanti del cabinet!
Quindi, per esempio l'"1UP" (giocatore uno) che nell'emulazione mame si ottiene premendo il tasto "5" sulla tastiera, dovrà essere generato dalla pressione del pulsante "1UP" sul cabinato... Una soluzione potrebbe essere quella di tagliare i cavi che vanno al connettore JAMMA, smontare la tastiera, trovare i fili giusti e quindi collegarli direttamente alla tastiera, aprendola e saldandoli sullo stampato, in modo da far chiudere il contatto corrispondente al tasto "5" alla pressione del pulsante sul cabinato.
Fortunatamente esiste una soluzione molto più comoda, che si chiama J-Pac. Si tratta di una schedina prodotta dalla ultimarc (www.ultimarc.com), alla quale si attacca da un lato direttamente il connettore jamma, e dall'altra la tastiera (in by-pass) e l'uscita della scheda video. Fine degli sbattimenti.
La schedina, tramite il connettore JAMMA, "sentirà" quali pulsanti sono stati premuti sul cabinet, quindi produrrà il codice giusto da inviare al computer tramite il cavo tastiera. Esiste un "mapping" tra i pulsanti del cabinet e l'equivalente codice tastiera da generare che è nella schedina stessa e può essere anche riprogrammato a piacere. Ma di solito può andare bene così come è. Costa 57$ + 12 $ per la spedizione.
Per quanto riguarda l'audio, vi consigliamo di smontare le casse originali del cabinet e di inserirne alcune (amplificate) di media fattura, che andrete a collegare direttamente all'uscita della scheda audio del PC. Meglio se usate casse stereo, visto che sono molti i giochi a utilizzarlo.
Come sistema operativo si può utilizzare windows 98 per la formattazione dei dischi (VFAT32 permette di superare il limite dei 2 GB, visto che una collezione completa di Rom ormai occupa quasi 7 Gbyte), per poi utilizzarlo in modalità DOS per far partire la vostra Mame machine.... in bocca al Pac-Man!

Guglielmo Cancelli e SpeedyNT

CONFIGURARE IL PC

A seconda che si voglia utilizzare Mame oppure Windows, sarà necessario caricare impostazioni diverse all'avvio del computer. Meglio automatizzare il tutto con questi file di configurazione ad-hoc.

```
CONFIG.SYS

[menu]
menuitem=mame, MAME
menuitem=win98, WIN98
menudefault=mame,2

[mame]
dos=high,umb
device=c:\windows\himem.sys

[win98]
device=c:\windows\himem.sys


AUTOEXEC.BAT

@echo off
goto %CONFIG%

:mame
rem mode con codepage prepare=((850)
C:\WINDOWS\COMMAND\ega.cpi) rem mode
con codepage select=850
rem keyb it,,C:\WINDOWS\COMMAND\key-
board.sys mode con rate=32 delay=1
keyb it
c:\doscfg\ctcm.exe >nul
c:\awedosdr\mixerset.exe /MA:200
cd \doscfg\fastvid
fastvid 111 16 e0000000 >nul
c:\windows\smartdrv 4096 >nul
cd\mame
advmenu
goto end

:win98
c:\windows\win

:end
```

RESUSCITATE UN VECCHIO PC!

Come riutilizzare hardware obsoleto con GNU/Linux o con altri sistemi liberi

In seguito alla costante diminuzione dei prezzi dell'hardware, a partire dalla seconda metà degli anni '90 **si è venuta ad accumulare una mole impressionante di computer vecchi e inutilizzati**. Lo scopo di questo articolo è offrire ai lettori alcune informazioni utili per riutilizzare questo hardware obsoleto con GNU/Linux o con altri sistemi operativi liberi.
In particolare verranno analizzate l'installazione e la configurazione del sistema operativo, accompagnate da un breve excursus sulle varie possibilità di utilizzo della macchina appena recuperata

>> Cosa si può fare

D'accordo, nessuno pretende di usare un vecchio Pentium I per fare grafica, giocare o come macchina per la riproduzione di video, però sono molti gli scopi per cui un vecchio PC può essere rimesso al lavoro.
Un 386 o un 486 con due schede di rete possono essere usati per **fare da router e firewall**, permettendo di collegare diversi computer in rete attraverso una sola connessione Internet. Un Pentium I dotato di scheda audio, per esempio, può essere collegato allo stereo e **trasformato in un jukebox per Mp3**. Se ha anche una scheda di rete, poi, non c'è nemmeno bisogno di un monitor: lo si può comandare da un qualsiasi PC collegato da un'altra stanza. Un vecchio PC con hard disk piuttosto grandi, **può fungere da file server**, ed essere usato come serbatoio per i file ingombranti (utilissimo per chi usa un portatile come computer principale), o **fare da server di stampa** per un piccolo ufficio. Le possibilità sono infinite, e sono determinate solamente dalle vostre necessità e dalla vostra creatività.

>> La scelta del sistema operativo

Se avete una macchina di classe 80286 o inferiore (non verranno trattate le architetture non x86), la scelta si riduce a tre sistemi operativi : **ELKS**, **Minix** e **FreeDOS**.
ELKS è l'acronimo di Embeddable Linux Kernel Subset, vale a dire una versione ridotta di Linux in grado di girare su sistemi a 16 bit. Il progetto ha raggiunto un buon grado di sviluppo e la sua home page è http://elks.sourceforge.net
Minix nacque dalla mente di Andrew S. Tanenbaum come una versione semplificata di Unix per uso didattico. Attualmente è giunto alla versione 2.0 e la sua home page è: www.cs.vu.nl/~ast/minix.html.
FreeDOS è un'implementazione libera di MS-DOS ed è in uno stato avanzato di sviluppo. È compatibile con la maggior parte delle applicazioni per il DOS di Microsoft e lo potete trovare su www.freedos.org.
Utilizzando una macchina a 32 bit di classe 80386 o superiore la scelta ideale diventa GNU/Linux.
Se le risorse disponibili sono scarse (< 300 MB di disco, < 16 MB di RAM), dovrete rivolgervi a mini-distribuzioni come muLinux (http://mulinux.sunsite.dk) o SmallLinux (http://www.superant.com/smalllinux), due prodotti tecnicamente molto validi.
Se invece non avete problemi con le risorse di sistema (per esempio un 486 con 16 Mbyte di RAM e 500 Mbyte di disco), potete utilizzare distribuzioni come Debian o Slackware. Nelle prove utilizzeremo Debian per via della comodità di gestione del sistema dei pacchetti tramite APT. Le procedure descritte sono applicabili a qualsiasi distribuzione.

>> Il target di utilizzo della macchina

Naturalmente, il target di utilizzo della macchina che andremo a configurare varia in base alle risorse che essa ci offre.

• **Per i processori di classe 80286 o inferiore**, si potrà ottenere un sistema Unix minimale, in grado di offrire al massimo un server HTTP (ELKS, Minix), FTP (Minix) o POP3/STMP (Minix). Sarà possibile collegare la macchina in rete attraverso i protocolli SLIP (ELKS, Minix), PLIP o Ethernet (Minix).

• **Per i processori di classe i386 ed eventualmente i486** con pochissime risorse, si può realizzare un router/firewall utilizzando la mini-distribuzione Linux Router Project (www.linuxrouter.org), che però è stato dichiarato morto il 22 Giugno di quest'anno. In alternativa è possibile utilizzare una mini-distribuzione (vedi sezione precedente) ed avere un sistema Linux di base per lavorare.

• Su macchine un po' più recenti (processori di classe **Pentium o superiori**) è possibile realizzare delle piccole stazioni multimediali in grado di riprodurre flussi audio/video anche su dispositivi esterni come televisioni.

In ogni caso in questo articolo analizzeremo solamente l'installazione e la configurazione di un sistema di base, poichè trattare ogni ambito di utilizzo descritto richiederebbe molto spazio e sarebbe inutile vista la grande quantità di documentazione disponibile in rete.

>> Installazione di Debian GNU/Linux

Nelle prove utilizzeremo **i primi due cd-rom di Debian 3.0 Woody**: se non li avete potete scaricarli da www.debian.org (**figura 1**). Poiché molti computer vecchi non supportano il boot da cd-rom, dovrete avviare il sistema con un floppy di boot e lanciare lo script AUTOBOOT.BAT dalla cartella DOSUTILS del primo cd-rom.

FIGURA 1

Se non avete dimestichezza con fdisk ocfdisk, potete usare **Ranish Partition Manager** (www.ranish.com/part), che pero è un software proprietario. Per quanto riguarda la dimensione delle partizioni, vi consiglio di allocare almeno 64 MB (128 è il quantitativo ottimale) in una partizione Linux Swap, e lo spazio rimanente in una Linux ext2.

Ritornando all'installazione, con lo script **AUTOBOOT.BAT** userete un kernel 2.2 . Se avete particolari esigenze, potrete compilare un nuovo kernel oppure **creare un boot disk con il kernel 2.4 di Debian** (bf24). Per la maggior parte delle operazioni potete leggere le istruzioni a video, quindi descriverò solo sommariamente i passi da seguire.

Una volta avviata la procedura d'installazione dovrete selezionare la lingua (**figura 2**), configurare la tastiera e impostare le partizioni di swap e di root. Successivamente dovrete selezionare **i moduli del kernel da caricare automaticamente all'avvio**: generalmente potete utilizzare la configurazione di default. Poi bisogna configurare alcuni parametri di rete quali hostname ed indirizzo IP (se è presente una scheda ethernet). Verrà installato un sistema di base e vi verrà chiesto di renderlo avviabile tramite il disco fisso o un floppy: scegliete quest'ultima soluzione solo in sistemi dual-boot, per poter configurare successivamente il boot loader di sistema.

FIGURA 2

Una volta riavviato il computer si avvierà il tool di Debian per la **seconda fase dell'installazione**: qui dovrete selezionare la vostra Time Zone, impostare una password per root e creare eventualmente un utente normale; successivamente dovrete effettuare uno scan dei cd di installazione. Ricordatevi di **rispondere no alle due domande** relative all'installazione via PPP e al download degli aggiornamenti di sicurezza. Ora dovrete selezionare alcuni dei gruppi di pacchetti presenti in taksel (**figura 3**) : personalmente consiglio di installare solo X Window System, Dialup System ed eventualmente gli ambienti per C and C++, Python e Tcl/Tk.

FIGURA 3

La scelta dovrà basarsi principalmente sulle vostre necessità e sullo spazio disponibile sul disco.

Ricordatevi di **rispondere negativamente** alla domanda relativa a dselect. Ora inizia la fase di installazione vera e propria. Vi verranno poste alcune semplici domande : vi consiglio di generare it_IT e it_IT@euro per i locales, di disabilitare SSH all'avvio e di saltare la configurazione di X che verrà eseguita in un secondo momento. Durante l'installazione vi verrà

I PACCHETTI DA INSTALLARE

Pacchetto	Descrizione
abiword	Word processor completo e leggero
abiword-doc	Documentazione per AbiWord
abiword-plugins	Plugins per AbiWord
ash	Shell adatta per sistemi con poca RAM
alien	Strumento per la gestione dei pacchetti
aumix	Gestione del mixer della scheda audio
blackbox	Window Manager spartano ma veloce
bzip2	Utility per la gestione dei file compressi .bz2
esound	Server sonoro di Enlightenment
gimp1.2	Il programma di grafica per eccellenza
gnumeric	Foglio di calcolo in stile Microsoft Excel
libgtk1.2	Librerie GTK+
libqt2	Librerie QT
links	Browser testuale
mc	File Manager in stile Norton Commander
mpg321	Strumenti per la riproduzione di files MP3
timidity	Riproduttore di file MIDI
tin	News reader
wmaker	Window Manager completo e leggero
wmakerconf	Tool di configurazione per WindowMaker

chiesto ogni tanto di sostituire il cd-rom nel lettore. Al termine del processo vi si presenterà il prompt per il login : accedete al sistema come utente root.

>> Configurazione di Debian GNU/Linux

La distribuzione Debian ha una configurazione di default **non perfetta per i nostri scopi**, quindi cominciamo a smanettare sul nostro nuovo sistema.
Per prima cosa occorre personalizzare la procedura di avvio: Debian in tutti i runlevel carica molti servizi inutili, quindi ne elimineremo alcuni. Cominciamo dal runlevel 2. Entrate nella cartella /etc/rc2.d/ e digitate :

```
# rm S19nfs-common S20diald
S20exim S20irda S20isdnutils
S20lpd S20pcmcia S20wwwoffle
S20xfs S99fetchmail   S99xdm
S99gdm
```

La voce relativa a gdm può anche non essere presente.
Rieseguite lo stesso comando per le cartelle /etc/rc3.d/ e /etc/rc4.d/; per quanto riguarda il runlevel 5, entrate in /etc/rc5.d/ e digitate :

```
# rm S19nfs-common S20diald
S20exim S20irda S20isdnutils S20lpd
S20pcmcia S20wwwoffle S99fetchmail
```

In questo modo il runlevel 5 sarà l'unico ad eseguire automaticamente X.
Ora bisognerà configurare il server grafico : avviate xf86config (figura 4) e seguite le istruzioni a schermo. Successivamente dovranno essere installati alcuni pacchetti non previsti di default : basta digitare "apt-get install" seguito dai loro nomi (tabella 1).
Ci sono ancora tanti piccoli accorgimenti per velocizzare il sistema : qui tratterò solo quello relativo alle VCs. Potete trovarne altri leggendo il 4mb Laptops HOWTO e lo Small Memory mini HOWTO che ho tradotto un po' di tempo fa e che sono disponibili all'indirizzo http://members.xoom.it/pctips2/HOWTO/italian/

Le VCs (Virtual Consoles) sono le classiche console che siamo abituati ad usare con Linux in modalità testuale. Poiché generalmente sono 6 ed un utente medio ne usa al massimo 3, esiste un modo per limitarne il numero e liberare così parecchia memoria.

FIGURA 4

Aprite il file /etc/inittab e posizionatevi su questo paragrafo :

```
# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
```

Per ridurre il numero di VCs basta mettere all'inizio di ogni riga un # (in gergo commentare), partendo dal basso verso l'altro. Ogni riga commentata equivale ad una VC in meno. Salvate il file e riavviate il sistema.

Dopo un po' vi si ripresenterà la schermata di login : inserite i vostri nome utente e password e inizate a divertirvi !!!
Per entrare in modalità grafica bisogna digitare da root "init 5" o semplicemente "startx". Vi consiglio di usare un window manager leggero come WindowMaker o BlackBox. Per sceglierne uno come predefinito basta creare un file chiamato ".xinitrc" nella vostra home directory contenente il comando per lanciare il vostro window manager (Es. "wmaker").

pctips
pctips@hardwaretips.com

FORMAT STRING, UN BUG MOLTO DIFFUSO

Molti programmi sono vulnerabili a un tipo di attacco basato sull'inserimento di parametri e codici di controllo all'interno di una maschera di input. Scopriamone tutti i dettagli.

La format string è una vulnerabilità relativamente "nuova": ufficialmente risale alla seconda metà del 2000, anche se si pensa che exploit del genere **circolassero nell'underground già da circa un anno**. In questo articolo andiamo ad esaminare in cosa consiste questa vulnerabilità, cosa ci permette di fare e come può essere sfruttata. Per questioni di spazio l'articolo è molto sintetico, **ma troverete spiegazioni dettagliate ed i sorgenti di esempio nella sezione "contenuti extra" del sito di HJ**.

>> Inquadriamo il problema

Per iniziare a capire il problema, prendiamo in esame la **funzione printf**, usata quasi in tutti i programmi scritti in C (ricordiamo però che sono vulnerabili tutte le funzioni che usino una stringa di formattazione). Questa funzione ci permette di visualizzare in una forma leggibile dall'utente un dato appartenente ad uno dei tipi fondamentali del C. Per esempio un intero chiamato **'a'** a cui assegniamo il valore **11**, in memoria è rappresentato da una word di 4 byte contenente il valore esadecimale **0x0000000b**. Per stampare il valore di **'a'** dobbiamo trasformarlo in una stringa contenente i caratteri **"11"**. In questi casi utilizziamo la funzione **printf**, che richiede un numero variabile di parametri di cui uno deve necessariamente essere un puntatore ad una stringa che chiameremo **stringa di formattazione**.
Un esempio:

```
printf("Il valore di a è:
%d\n",a);
```

Abbiamo passato due parametri: il primo è la **stringa** e il secondo è l'intero **a**. La funzione printf stampa la stringa finché non trova il carattere **%** che indica che vogliamo stampare il valore di un parametro mentre il carattere successivo (dopo %) dice alla funzione **in che formato vogliamo visualizzarlo**. Il parametro viene convertito in una stringa adeguata e stampato. Nel nostro caso printf **stampa tutti i caratteri fino ad arrivare a %d**: qui capisce che vogliamo stampare un parametro rappresentandolo come un numero decimale (la 'd' dopo il '%' significa appunto numero decimale), quindi la variabile **a** viene trasformata nella stringa "**11**" e stampata. L'output sarà:

```
Il valore di a è: 11
```

La funzione mantiene sempre un puntatore interno che si riferisce al prossimo parametro da interpretare e i parametri si trovano sullo stack dopo la stringa. **E se provassimo a stampare parametri che non abbiamo passato?** La funzione visualizzerebbe i valori presenti dopo la nostra stringa, **permettendoci di leggere lo stack**. E sullo stack ci sono anche gli indirizzi di ritorno delle funzioni... non vi viene in mente che **qualcosa di pericoloso potrebbe accadere?**

Difficilmente troveremo mai un errore di programmazione così grossolano, e comunque non darebbe la flessibilità necessaria a mettere in atto un attacco. Ma cosa succederebbe se in qualche modo **l'input dell'utente modificasse la stringa di formattazione?** Beh, sarebbero guai grossi...

>> Il bug al lavoro

Ora vediamo in linea generale come possiamo sfruttare la vulnerabilità, in modo da semplificare la comprensione dei programmi di esempio.
Immaginiamo di avere un programma in cui **l'utente passi completamente la stringa di formattazione, come il programma di esempio.** Inserendo questo input:

```
%x
```

verrà visualizzata la conversione in esadecimale del valore presente nello stack dopo la nostra stringa.
Se invece diamo:

```
%x.%x.%x.%x.%x
```

otterremo i 5 valori successivi alla stringa, separati da un punto. Ma **se volessimo vedere cosa c'è 200 posizioni dopo?** Sarebbe noioso e l'input potrebbe essere troppo lungo. Come facciamo? Esiste un costrutto accettato da quasi tutte le librerie C, che permette di accedere direttamente ad ogni parametro mettendo il numero di parametro che vogliamo usare seguito dal carattere **$** tra il **%** e il carattere che definisce il formato. **Per vedere il 200esimo parametro in esadecimale diamo questo input:**

```
%200$x
```

Bene, **possiamo praticamente leggere tutti i valori nello stack dalla posizione corrente fino alla cima**. Sfruttiamo questa opportunità e leggiamo un po' di parametri.

>> Sempre più pericoloso

Possiamo cercare degli indirizzi di ritorno da sovrascrivere e il buffer che contiene il nostro input, in modo da **poterci inserire eventualmente uno shellcode**. Un indirizzo di ritorno (che per comodità chiameremo **RETADDR**) in genere è accoppiato con un frame pointer, quindi cerchiamo una coppia di valori in cui uno inizi con **0xbffff** e uno con **0x08048**. Questo perché su macchine Linux lo stack inizia all'indirizzo **0xbffff000** e lo spazio in cui possiamo mettere del codice da eseguire inizia da **0x08048000**.
Poiché i buffer statici sono dichiarati all'inizio di una funzione, probabilmente troveremo questa coppia di valori subito dopo il nostro buffer. Trovato il buffer e la coppia di valori, facendo un semplice calcolo (ogni parametro occupa **4 byte**) possiamo capire a che distanza dal buffer si trovi il RETADDR. Però non sappiamo quale sia l'indirizzo reale del buffer, e quindi abbiamo due opzioni: **trovarci l'indirizzo o scrivere un exploit che provi tutti gli indirizzi**.
L'indirizzo del buffer sarà probabilmente sullo stack essendo stato passato a qualche funzione, quindi sarà uno degli indirizzi **0xbffff** che troviamo, ma quale? C'è un modo per leggere da un indirizzo. Oltre a **%d** ci sono altri descrittori di formato accettati da printf, e per noi i più interessanti sono **%u**, **%n** (che verranno esaminati dopo) e **%s**. Quest'ultimo visualizza una stringa, puntata dal parametro dato. Se ad esempio il parametro 3 è un indirizzo sospetto, diamo questo input:

```
%3$s
```

il risultato è una stringa letta dall'indirizzo che si trova come parametro 3. Se questa è proprio la nostra stringa di input abbiamo trovato l'indirizzo del buffer e potremmo pensare di scrivere un

UN PROGRAMMA VULNERABILE

Questo è un esempio di programma volutamente vulnerabile al bug della format string. Potete usarlo per i vostri esperimenti.
Salvatelo sulla vostra Linux box come format.c e compilatelo con gcc -o format format.c
Il sorgente lo trovate anche nella sezione Contenuti Extra del nostro sito, con molte spiegazioni aggiuntive e a un exploit di esempio.

```
/* #format.c# Programma vulnerabile alle format string
   scritto da gufino2 per Hacker Journal */
#include<stdio.h>
void func(char *sm){
      char buffer[100];
      bzero(&buffer,100);
      strncpy(buffer,sm,100);
      printf(buffer);
}
int main(int argc, char **argv){
      if(argc<2){
            printf("Usage: ./format <string>\n");
            exit(-1);
      }
      func(argv[1]);
      printf("\nFatto\n");
}
```

LA BIBBIA DEL FORMAT STRING BUG

L'articolo del Team Teso sull'exploit delle stringhe di formattazione lo potete trovare, in inglese e completo dei sorgenti, all'indirizzo:

http://www.team-teso.net/articles/formatstring/

exploit "mirato".
In realtà **questo potrebbe non andare bene**, perché gli indirizzi possono cambiare ad ogni esecuzione del programma. Spesso è più affidabile un exploit che provi tutti gli indirizzi.

>> Sovrascrivere dati

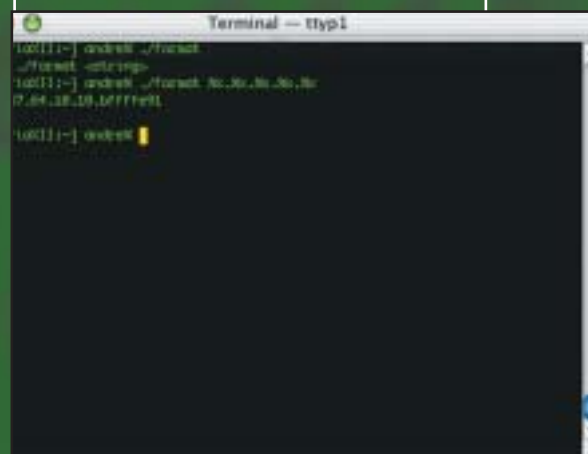
Passiamo alla sovrascrittura: come possiamo scrivere in una determinata locazione? Fra i descrittori di formato ne troviamo uno molto particolare, che è **%n**: questo descrittore non visualizza niente, ma scrive il numero di caratteri stampati finora nell'indirizzo che gli diamo come parametro. Per forzare **%n** a scrivere dove vogliamo noi, basta passargli l'indirizzo su cui scrivere, e lo passeremo sulla stringa. Se l'inizio del buffer è al parametro **8**, dando una stringa del tipo:

```
char
stringa[]="\x44\x43\x42\4x1%8$n";
```

scriveremo il valore 4 all'indirizzo **0x41424344** che abbiamo passato sulla stringa in formato little-endian.
Bisogna anche riuscire a comandare il valore che verrà memorizzato. Alcuni descrittori di formato accettano tra il **%** e il carattere un numero decimale che indica con quanti caratteri scrivere il valore riempiendo i caratteri in eccesso con spazi. Per i nostri scopi useremo **%u** che scrive un numero **unsigned**. Possiamo aumentare il numero di caratteri scritti in maniera arbitraria, ma per evitare problemi con alcune librerie C ci limiteremo a forzare **poco più di 255 caratteri**. Se ci proviamo, noteremo che **%n** scrive comunque 4 byte, il che significa che in una architettura little-endian sovrascriviamo in pratica **solo il byte meno significativo**, azzerando gli altri 3. Per sovrascrivere un RETADDR useremo 4 scritture a indirizzi consecutivi, scrivendo **un byte alla volta**. Questa situazione risolve anche un altro problema: cosa succede infatti se dobbiamo scrivere un valore **minore del numero di caratteri già stampati?** Sappiamo che ci interessa scrivere solo il byte meno significativo; degli altri ci occuperemo successivamente. Se abbiamo già scritto **0x000a** (dieci) caratteri e il prossimo valore da scrivere è **0x0009** basta fare in modo che il numero di caratteri scritti arrivi a **0x0109**. Dobbiamo anche ricordare che **non possiamo stampare un valore con un numero di caratteri inferiore a quelli necessari**, quindi se vogliamo scrivere 3 caratteri ma il valore è a 4 cifre dobbiamo forzare **non 3, ma 256+3 caratteri**.

>> In definitiva...

Ora siamo in grado di provare un attacco. Sappiamo che abbiamo un buffer e che il RETADDR da sovrascrivere si trova un certo numero di byte più in su. Dobbiamo passare una stringa che contenga le 4 sequenze atte a mettere nel RETADDR l'indirizzo del nostro shellcode, che si trova subito dopo sulla stringa. Visto che non possiamo sapere l'indirizzo del buffer ci tocca scrivere un programma che provi tutti gli indirizzi e per ognuno costruisca la stringa "maliziosa" e la invii.
Ci sarebbe ancora molto da dire sulle format string, e parlare di casi in cui dobbiamo usare approcci diversi.
Quindi sto preparando una traduzione del documento pubblicato dal TESO GROUP, che è una piccola bibbia della format string. Appena la traduzione sarà finita indicherò l'URL sul forum di HJ. Nel frattempo spero che questo articolo vi abbia dato le basi per individuare ed evitare questa vulnerabilità nei vostri sorgenti.
Per rendere i nostri programmi meno vulnerabili a questo attacco: la regola fondamentale è di definire sempre la stringa di formattazione nelle funzioni vulnerabili, e porre molta attenzione a tutti i punti del programma in cui visualizziamo stringhe fornite dall'utente.

> **Little-endian**
> Un'architettura di computer in cui, data una word di 16 o 32 bit, i bit all'indirizzo più basso sono quelli meno significativi (little-end-first). Il termine viene anche usato per descrivere l'ordinamento di unità diverse dal byte (spesso, i bit all'interno dei byte).

Il programma format.c in esecuzione, con uno degli esempi citati nell'articolo. Piccola nota: il programma si compila e funziona anche su Mac OS X.

Per esempio per stampare una stringa che si trova nel buffer stringa_utente dobbiamo fare:

```
printf("%s",stringa_utente);
```

invece di:

```
printf(stringa_utente);
```

Se poi volete far verificare i vostri programmi, ho creato un canale Irc dedicato alla sicurezza, e in particolare all'auditing dei sorgenti (sia per chi vuole iniziare che per chi è già un pò più smaliziato). Il canale è **#auditers** e si trova sul server di Azzurra, lo stesso di **#hackerjournal**.

Piergiorgio Cardone a.k.a. gufino2
busgman@libero.it

Il mio nome è LINUX, XBOX LINUX

Grazie a un bug nel gioco "007 Agent Under Fire" è possibile eseguire Linux su una console XBOX non modificata.

XBOX Linux Project (http://xbox-linux.sourceforge.net/) è un audace progetto che cerca di **creare una versione di GNU/Linux che possa funzionare appieno sulla console della Microsoft XBOX**. Il loro intento però è di **rimanere completamente nella legalità**, quindi non vogliono ricorrere ai modchip o ad altri metodi che possano compromettere l'integrità della console, affidandosi unicamente a software legali o privi di copyright e al reverse engineering applicato al software di sistema della console in conformità con le leggi locali.

>> Un progetto, due fasi

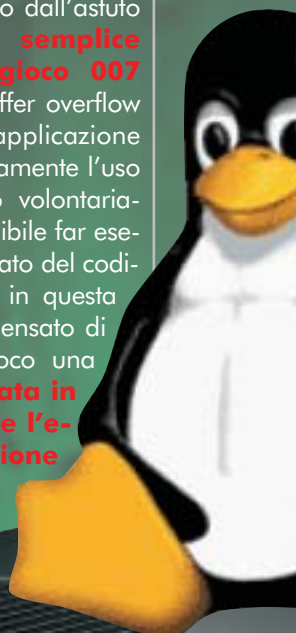
Lo sviluppo di quest'idea si suddivide in due parti: A e B. **Il progetto A produrrà le parti principali del nuovo software**, ovvero un rimpiazzo per il BIOS e una distribuzione Linux completa di kernel, l'ambiente grafico X-Window con KDE o Gnome e un bootloader. È ovviamente previsto il supporto totale delle periferiche XBOX, quindi Linux potrà usufruire liberamente dell'hard disk, del drive DVD, dell'interfaccia network, delle porte USB e di ogni hardware a esse connesso. Per usufruire al meglio di Linux ci sarà bisogno di altre periferiche USB o a infrarossi come per esempio tastiera, mouse, un adattatore VGA per poter collegare la console a uno schermo. Una delle potenzialità che trovo più allettanti è la futura possibilità di far girare **qualsiasi altro sistema operativo o console** attraverso emulatori o Virtual Machine, come ad esempio VMware o Plex86 per Windows 2000/NT e altro.

Il progetto B ha il delicato compito di trovare un metodo per usufruire in toto dell'XBOX senza modifiche hardware alla stessa. Come potete immaginare questo non è affatto semplice; finora era stato possibile aggirare il problema delle informazioni cifrate (RSA a 2048 bit, un cifrario a chiave pubblica basato su un procedimento che sfrutta le proprietà dei numeri primi) solo attraverso l'istallazione di un modchip.

>> L'uovo di colombo

Il 29 marzo, habibi_xbox pubblica la sua scoperta su XboxHacker.net, uno dei più famosi forum del settore. La prima soluzione del Project B Competition appare pubblicamente e XBOX Linux Project conferma la sua validità due giorni dopo. Il mezzo usato dall'astuto habibi_xbox **sfrutta un semplice buffer overflow del gioco 007 Agent Under Fire**. I buffer overflow avvengono quando un'applicazione non riesce a gestire correttamente l'uso della memoria; causando volontariamente tale processo è possibile far eseguire al programma attaccato del codice arbitrario. Esattamente in questa maniera habibi_xbox ha pensato di far caricare all'ignaro gioco una partita registrata, **modificata in maniera da permettere l'esecuzione di una versione di Linux**.

A quanto ci dice il primo vincitore del Project B Competition, 007 Agent Under Fire non è affatto l'unico gioco soggetto a tale bug. La scelta di habibi_xbox è rica-

duta su questo titolo solo perchè a quanto pare è in grado utilizzare lo stesso gioco salvato senza problemi di compatibilità, sia in versione PAL che in versione NTSC.
Vediamo la spiegazione punto per punto di come lanciare Linux sulla vostra console mai aperta. Vi avverto che è un metodo funzionante ma altamente complesso, sperimentale e incompleto. Questa soluzione non permette ancora di godere appieno di Linux con la vostra XBOX non modificata, **ma è solo un primo risultato che come la prima breccia in un muro permetterà di abbatterlo**.

>> Cosa serve

1) Una console XBOX della Microsoft **mai modificata** (il funzionamento di questo metodo non è garantito su un XBOX con modchip).
2) Un PC disponibile.
3) Il gioco originale **007 Agent Under Fire** della Electronic Arts, da non confondere con 007 NightFire.
4) La versione ISO della piccola distribuzione di **XBOX Linux Project** chiamata "XBOX Linux Live" (http://xbox-linux.sourceforge.net/download.php).
5) Un metodo che permetta di **trasferire un savegame dentro una memory card**. Questo è fattibile in diversi modi, come ad esempio i pezzi hardware di xbox-saves.com, o un cavo USB-XBOX oppure una memory card standard se vi è possibile copiarci dentro dei files.
6) **Un savegame per il gioco in versione txt** reperibile sempre da Xbox Linux a questo indirizzo http://xbox-linux.sourceforge.net/down/007linux.txt.

Michael Robertson, fondatore e CEO di Lindows, promise di premiare con 100.000 dollari il completamento di ognuna delle due fasi e proprio da questo venne fuori l'idea di una gara a premi. Project B Competition infatti non è altro che questo: una gara in cui gli hacker più veloci e astuti si sfidano cercando di trovare una falla nel software dell'XBOX che permetta di lanciare programmi non ufficiali e di raggiungere il controllo della console; a seconda della completezza della soluzione, il fortunato hacker riceverà tutti o una parte dei soldi messi in palio da Mr. Lindows.

>> La preparazione

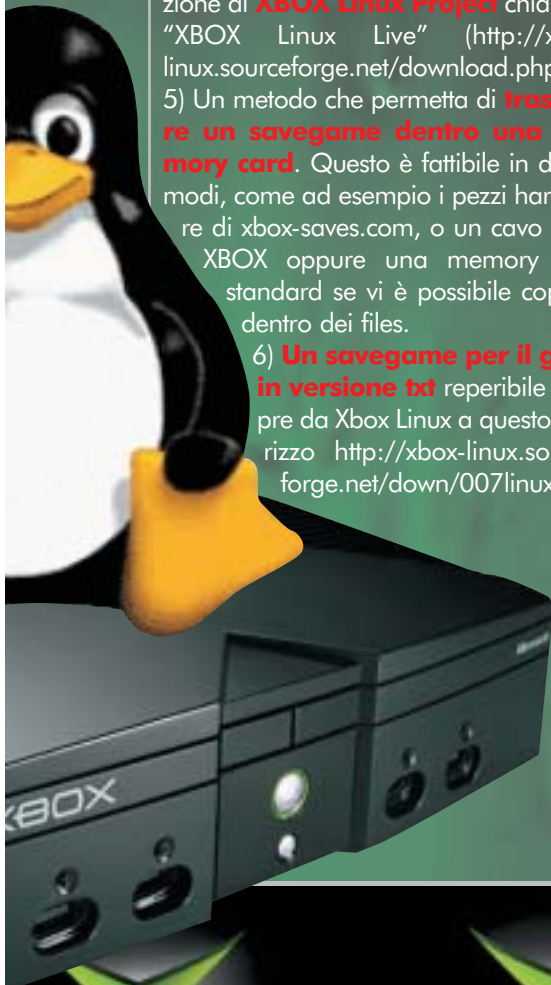
Iniziamo preparando il savegame (il gioco salvato) e riportandolo alla sua forma originaria. Come potete ben notare aprendo il txt, infatti, non assomiglia per niente a un testo ascii. In verità il file è un archivio zip codificato mediante il protocollo UUencode. Per decodificare il file avete diverse possibilità: la prima e più semplice è di rinominare il file 007linux.txt in 007linux.uu per poi aprirlo con **WinZip**; la seconda possibilità invece è quella di usare un programma specifico per decodificare tale tipo di protocollo come ad esempio **uudecode** reperibile per DOS, Windows e Linux o **uutool** per Mac. Poi scompattate lo zip.
A questo punto avete bisogno di un programma per estrarre i dati da dentro un'immagine ISO, come ad esempio WinISO da Windows o il pratico mount da Linux. Copiare tutti i file estratti dall'ISO di Linux dentro la directory

```
UDATA/4541000d/000000000000/
```

precedentemente estratta dallo zip. Ricordatevi di includere la sottodirectory boot alla copia, ma non il file plugin.img perché altrimenti lo spazio di una normale memory card potrebbe non essere sufficiente a contenere tutto. Ora facciamo attenzione al file default.xbe. Dobbiamo sostituire i sui primi bytes **0x380** con i bytes **0x380** contenuti nel file default.patch. Poi bisogna copiare i dati dentro la memory card: copiate la directory **4541000d/** e tutto il suo contenuto (comprese le sottodirectory), ma non la **UDATA/** che in verità è stata inserita unicamente per facilitare l'utilizzo dei software di copia di xbox-saves.com.

>> La pratica sulla console

Per prima cosa bisogna inserire la memory card nell'XBOX e copiare il savegame di 007 dalla card al hard disk, tramite il dashboard della console.
Inserire il gioco 007 Agent Under Fire nella console e lanciare il gioco. Poi, attraverso il menù principale scegliere "Load Mission" e subito dopo "XBOX Hard Disk". **A questo punto il gioco è fatto!** Se tutto è andato a buon fine, a questo punto dovrebbe apparirvi una schermata completamente nera, poi il LED dovrebbe diventare arancione (sintomo che il kernel di XBOX Linux Live è stato caricato) e infine dovreste sentire i suoni di avvio di XBOX Linux Live.
Purtroppo lo schermo rimarrà nero perché in Linux il video deve essere inizializzato per funzionare, ma questo difetto potrebbe essere ovviato con Xromwell o, come consiglia XBOX Linux nel sito, attraverso l'utility xbv.
Con questo si conclude la spiegazione e come ultima nota vorrei ricordare che **non è possibile usare questo trucchetto per usufruire di giochi copiati** o altro con la console non modificata, funziona solo con XBOX Linux.

darkestsin

Scambiare dati su Internet con livelli di sicurezza

In questo articolo parleremo delle Virtual Private Networks (Reti Private Virtuali) intese come insieme di dispositivi, protocolli e servizi utilizzati principalmente dalle aziende per rendere disponibili ai propri collaboratori esterni o a sedi distaccate **dati riservati della propria rete lan, facendoli passare attraverso Internet**.
Naturalmente una pratica di questo tipo solleva non poche problematiche di sicurezza, che saranno appunto l'argomento di questo e del prossimo articolo. Poiché l'argomento è eccessivamente vasto daremo parecchi riferimenti tra i link e, dopo una breve descrizione della struttura di una VPN, ci concentreremo soltanto sul tunneling.

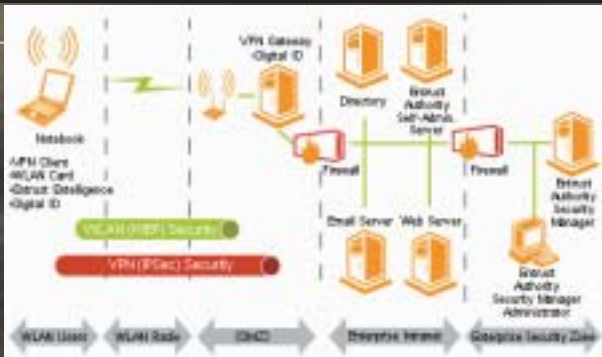
>> Struttura di una VPN

Elementi fondamentali di una VPN sono un **server PKI (Public Key Infrastructure)** che gestisca le politiche di sicurezza, un **gateway VPN** e, naturalmente, Internet.
La Public Key Infrastructure è una struttura modulare scalabile costituita dalle seguenti componenti:

• una o più **Autorità di Certificazione (CA)** che si occupano della gestione dei servizi di crittografia con la generazione e la distribuzione dei certificati a chiave pubblica, e gestiscono anche la durata dei certificati stessi attraverso la CRL (Lista di Revoca dei Certificati);
• un **servizio di directory** in cui sia contenuta la lista degli utenti del sistema con le relative politiche di sicurezza (un esempio di questo tipo è l'Active Directory di Windows 2000 Server);
• una serie di **applicazioni e servizi che utilizzino i sistemi crittografici a chiave pubblica**: servizio web con supporto SSL, servizio di posta che gestisca il protocollo criptato S/MIME, servizi di autenticazione criptata come Kerberos etc.

Se possiamo considerare quindi la PKI come il nucleo nella struttura di una VPN, i VPN Gateway possono essere considerati gli elementi di confine. I VPN Gateway sono quelle entità che creano il cosiddetto **tunnel su Internet per il transito protetto dei dati**. In realtà non viene creata una vera e propria corsia preferenziale percorsa dai pacchetti ma, come vedremo in seguito, **i pacchetti vengono criptati e incapsulati in pacchetti contenitore**. Quindi, nonostante seguano in rete vari percorsi come avviene per tutti gli altri pacchetti, sono leggibili esclusivamente dal destinatario.

>> Dispositivi hardware

Vi sono varie soluzioni per implementare un VPN Gateway. La prima soluzione è di utilizzare dei **dispositivi hardware**. A tal proposito esistono tre tipi di dispositivi che hanno utilizzi differenti:

Sito della Cisco, principale produttore di dispositivi VPN hardware

1. Concentratori VPN. Questi dispositivi vengono utilizzati per lo più nel caso in cui si voglia creare un collegamento tra agenti esterni che non si collegano sempre dallo stesso luogo o soggetti esterni all'azienda stessa, cioè quando si vuole creare un collegamento temporaneo. L'utente che utilizza il concentratore deve disporre di un client VPN hardware o software che in alcuni casi è in grado di gestire anche comunicazioni con dispositivi wireless. I concentratori gestiscono l'autenticazione degli utenti ed il criptaggio dei dati. Come esempio concreto potete dare un'occhiata ai concentratori Cisco della serie 3000 o 5000.
2. Router VPN. Vengono utilizzati per collegare tra loro sedi distaccate creando un collegamento stabile. In questo caso il collegamento avviene tra due router VPN e non tra un dispositivo che fa da server ed uno fa da client.

RETI PRIVATE VIRTUALI

paragonabili a quelli di una rete privata: possibile?

3. Firewall VPN. Hanno le stesse funzionalità dei dispositivi precedenti con in più le caratteristiche dei classici firewall.
L'utilizzo di questi dispositivi hardware non è necessario per mettere su una VPN, ma è possibile utilizzare un server con doppia interfaccia di rete che svolga le medesime funzioni di autenticazione degli utenti, cifratura dei dati e incapsulamento dei pacchetti. A tal proposito, nel box dei link trovate come implementare un VPN Gateway utilizzando Windows 2000 Server o Linux. Vi è inoltre un link che fa riferimento alle VPN nel nuovo Windows 2003.

>> Cifratura dei dati

Come abbiamo detto in precedenza, il tunneling operato dai VPN gateway si basa su **protocolli criptati**. È necessario però distinguere i protocolli utilizzati dai VPN gateway da quelli ai quali siete probabilmente più abituati, come ad esempio SSL per il web oppure SSH per il telnet. A differenza dei primi, infatti, **questi ultimi agiscono a livello applicazione del modello OSI**. Ciò significa che ad essere criptati sono esclusivamente i dati relativi ad una particolare comunicazione, come può essere quella tra noi e un server web, ma **il resto dei dati che escono ed entrano dal nostro sistema sono comunque in chiaro**. I protocolli utilizzati nei VPN gateway come l'IPSec agiscono invece a livello di rete del modello OSI, e ciò comporta quindi la **cifratura dell'intero traffico di rete**.

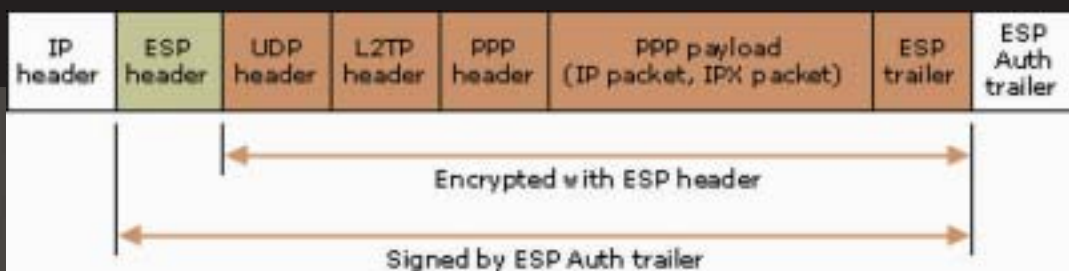
>> Comunicazioni blindate

Queste le principali problematiche di sicurezza che le VPN risolvono.

Bruce Schneier, crittanalista che ha esaminato i sistemi VPN di Microsoft.

L'intercettazione: se, infatti, un malintenzionato riesce ad intercettare i dati non potrebbe comunque leggerli e qualora cercasse di decrittarli non ci riuscirebbe in tempi utili.
L'autenticazione di un utente non autorizzato viene impedita attraver-

IPSEC, IL PROTOCOLLO SICURO

Il protocollo IPSec è il primo protocollo pubblico ideato per le VPN. Gli altri protocolli, infatti, come il PPTP o l'L2TP, sono proprietari. Come per gli altri protocolli pubblici che poi sono diventati degli standard di Internet, anche l'IPSec possiede le sue RFC reperibili presso il sito dell'IETF:
Nel box dei link trovate il sito del VPN Consortium in cui si può trovare un elenco completo degli RFC di IPSec. Prima però di inoltrarvi in una lettura così amena vi riporto il commento di uno dei più grandi esperti di sicurezza informatica e crittografia, Bruce Schneier, il quale nell'introduzione del suo scritto "Una valutazione crittografica di IPSec" scrive: "La nostra principale critica all'IPSec è la sua complessità. IPSec contiene troppe opzioni e troppa flessibilità; ci sono spesso svariati modi per fare le stesse cose o cose simili". Ciò che, infatti, ha lasciato interdetto non soltanto Bruce Schneier, ma tutta la comunità scientifica che si occupa di sicurezza informatica è proprio la quasi incomprensibilità degli RFC anche se sempre nella stessa introduzione Schneier aggiunge: "Nonostante tutto il serio scetticismo che nutriamo sull'IPSec, è probabilmente il migliore protocollo IP sicuro disponibile al momento".

L'incapsulamento dei dati nel protocollo L2TP.

so lo scambio di chiavi di sessione che serviranno a cifrare e decifrare i pacchetti

Riutilizzo dei pacchetti sniffati e modificati per dirottare le sessioni. Su questo punto è opportuno spendere qualche parola in più. Come qualcuno di voi saprà il concetto di spoofing dell'indirizzo ip si basa proprio sul dirottamento di una sessione attraverso la **generazione di pacchetti falsi che simulano la comunicazione legittima tra due nodi,** con lo scopo di inserirsi tra i due. Questa pratica viene evitata dal tunneling con la **generazione di un hash per ogni pacchetto di cui abbiamo parlato prima**. Infatti, una modifica al pacchetto comporterebbe un hash diverso e quindi una mancata corrispondenza tra il pacchetto è l'hash allegato e quindi un rifiuto del pacchetto da parte del gateway VPN.

>> La "Micosoft way"

Poiché all'IPSec dedicheremo il prossimo articolo, adesso spenderemo due parole per il PPTP di Microsoft e l'L2TP. Anche l'implementazione del PPTP utilizzata da Microsoft nei vecchi sistemi NT è passata al vaglio di Bruce Schneier (vedi box relativo all'IPSec), il quale nel suo documento **"Cryptanalysis of Microsoft's Point-To-Point-Tunneling Protocol"** scritto insieme a Mudge della L0pht (gli ideatori di L0phtcrack), mette in luce quelle che secondo lui sono le vulnerabilità di questo sistema.

Le VPN possono essere implementate nell'hardware di rete, in modo quasi trasparente per gli utenti.

Innanzi tutto, l'utilizzo del protocollo di autenticazione sicura MS-CHAP utilizzato dal PPTP si basa su **funzioni di crittografia di vecchia concezione,** che come nel caso di LanManager erano già state superate.
Alcune componenti delle chiavi di sessione erano ricavate dalle password degli utenti e quindi **avevano una lunghezza inferiore ai 40 e 128 bit dichiarati**.

Il canale di controllo (la porta TCP 1723) utilizzato per la negoziazione e la gestione delle connessioni **non era autenticato, ed era quindi vulnerabile ad attacchi di spoofing o DoS**.
Viene cifrato **soltanto il traffico dati** per cui un eventuale intercettatore potrebbe ricavare informazioni utili dall'analisi delle comunicazioni sul canale di controllo.
Maggior fortuna ha avuto invece l'**L2TP**, protocollo definito da IETF nell'RFC 2661 nato dall'unione del PPTP di Microsoft e del L2F di Cisco e ancora **utilizzato da Microsoft in Windows 2000 Server in accoppiata con l'IPSec**. Infatti, è possibile utilizzare l'L2TP per creare il tunnel cioè l'incapsulamento dei pacchetti, mentre IPSec si dedica alla crittografia dei dati. In figura potete vedere in che modo viene cambiata la struttura del pacchetto: l'header originale viene criptato e sostituito con un altro header.

Roberto 'dec0der' Enea

LINK UTILI

Se volete evitare di copiare a mano gli indirizzi, trovate i link nella sezione Contenuti Extra del nostro sito, nella Secret Zone.

http://www.vpnc.org
Il Virtual Private Network Consortium promuove l'utilizzo delle VPN e supporta gli standard IETF che le riguardano

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/vpnsol.asp
Pagina di TechNet di Microsoft in cui è descritta l'implementazione di una VPN su Windows 2000 server

http://www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.mspx
Pagine dedicate alle VPN nel nuovo server Windows 2003 di Microsoft

http://www.linux.org/docs/ldp/howto/VPN-HOWTO/index.html
How to per l'implementazione di una VPN con Linux

http://www.counterpane.com/ipsec.pdf
Link al documento originale di Bruce Schneier e Niels Ferguson "A Cryptographic Evaluation of IPSec".

http://www.counterpane.com/pptp.pdf
Link al documento originale di Bruce Schneier e Mudge "Cryptanalysis of Microsoft's Point-To-Point-Tunneling Protocol".

http://www.cisco.com
Sito della Cisco, principale produttore di dispositivi VPN hardware

Fai rivivere le cassette del C64 !

Come interfacciare il registratore del C64 al PC per trasferire i programmi su cassetta e usarli con un emulatore.

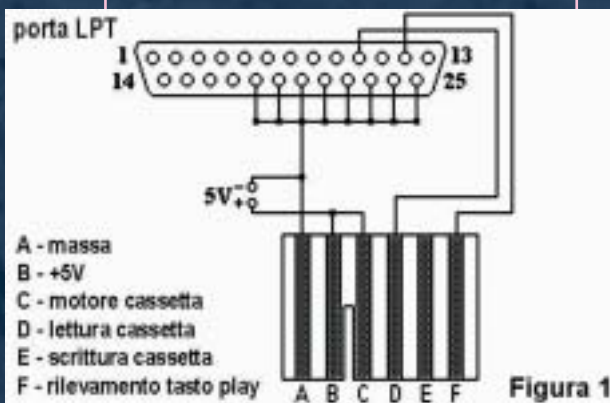
Avete una miriade di cassette del C64 e vorreste poterle utilizzare con un emulatore sul PC? Non è semplicissimo, ma si può fare. Bisogna innanzitutto **costruire un'interfaccia per poter collegare il datassette** (il registratore della Commodore) alla porta parallela del PC, per poi trasferire il contenuto delle cassette in appositi file .TAP da poter usare con l'emulatore. È ovvio che programmi di questo genere esistono già belli e pronti da scaricare (nonché interfacce da comprare), ma **perché non provare a programmarne uno tutto nostro**, che fa molto più figo? Bene, allora iniziamo a vedere come realizzare l'interfaccia.

>> L'interfaccia da costruire

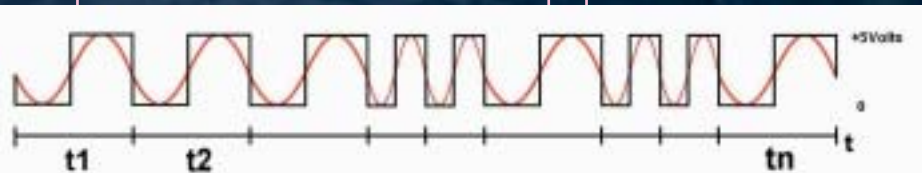
Il connettore del registratore presenta 6 contatti, una di massa, uno per i +5V di alimentazione della circuiteria, un'altro che porta sempre +5V al motorino per l'avanzamento del nastro, uno di rilevamento dello stato del pulsante play (premuto/nonpremuto) e due per la lettura e scrittura dei dati. Si intuisce subito che i dati in lettura, che poi sono quelli che a noi interessano, vengono trasmessi in modo seriale. Essi infatti viaggiano unicamente attraverso una singola linea. Inoltre, **avremo bisogno di un alimentatore per fornire la tensione richiesta**. Per iniziare, procuratevi un semplice connettore maschio da 25 poli (lo si può prendere da un cavo per stampante) e un qualsiasi circuito stampato (proprio qualsiasi) che presenti in un lato almeno una fila di 6 contatti di rame per connettori simili a quello del vostro datassette (di solito, dentro i vecchi televisori si trovano una quantità di schede a inserimento simili a cartucce delle console che potrebbero rivelarsi ottime). **Controllate che i contatti siano distanziati in maniera tale da coincidere più o meno con quelli del connettore** (è sufficiente che inserendolo non si presentino cortocircuiti), e se tutto risulta ok iniziate a ritagliare con un seghetto tale porzione di circuito togliendo di mezzo eventuali resistenze e compagnia bella, che possano dar fastidio. Fatto ciò, per evitare inserimenti errati e soprattutto per poter inserire fisicamente il connettore del datassette nel pezzo di circuito, **praticate un taglio sufficientemente largo tra il secondo e terzo contatto** in modo tale che, inserendo lo spinotto, vi sia continuità elettrica (ovviamente).

Per i +5V vi dovrete arrangiare ma un buon rimedio è quello di prelevarli dalla porta giochi della scheda sonora; la descrizione dei pin della porta giochi la trovate su www.computerrepairservice.com/cables/co_GameportPC.html

Non rimane che saldare svariati spezzoni di filo per creare il semplice circuito come in Figura 1. Per rimanere compatibili anche con altri software, la let-

tura dei dati sarà fatta dal pin 10 della LPT, mentre il rilevamento andrà sul pin 12.

Lo schema di collegamento tra il connettore del registratore del C64 e la porta LPT del PC.

>> Come interpretare i dati?

Il datassette registra i dati **sotto forma di toni** (utilizza normali cassette audio), ovvero di un segnale sinusoidale che cambia continuamente frequenza modulata in base ai bit che deve rappresentare.
La circuiteria non fa altro che porre sul piedino in uscita un'onda quadra (0Vo +5V) che rispecchia la sinusoide "letta" direttamente sul nastro, secondo lo schema in Figura 2. Siccome i dati sono codificati secondo la durata di ogni singola pulsazione (coppia basso-alto dell'onda quadra) si evince che in Figura 2 il segnale codifica la sequenza 111001001.

Come il registratore rappresenta i dati binari.

Quello che bisogna fare, mentre la cassetta "gira", è **registrare la durata di tali intervalli di tempo** qui denominati T1,T2 eccetera e registrarli in un apposito file compatibile con gli emulatori che ci sono in giro. Come si diceva prima tale file è un normale file TAP che ha questa struttura interna:

- **I primi 20 byte di header** contengono unicamente versione, dimensione del file e la frase ASCII "C64-TAPE-RAW".
- **I successivi byte** sono i dati veri e propri, e ogni byte rappresenta la durata di una pulsazione, secondo la formula: **DATA = (Fcpu) * (Tn) / 8**

dove **Tn** è la durata dell'ennesima pulsazione rilevata e **Fcpu** è la frequenza del processore del C64 (per la versione PAL del sistema tale frequenza vale 985248 Hz). Ogni pulsazione avente durata tale da generare un valore DATA maggiore di 255 viene scartata, e si pone il byte pari a zero. Per maggiori chiarimenti sulla struttura dei file TAP si può dare un'occhiata all'indirizzo: http://members.tripod.com/~petlibrary/TAP.HTM

>> Il programma

Per praticità, **il sorgente del programma è stato inserito nella sezione Contenuti Extra** della Secret Zone del sito di Hacker Journal; salvatelo in un file di testo, e tenetelo a portata di mano mentre leggete questa spiegazione.
Per poter misurare intervalli di tempo talmente brevi (dell'ordine dei 10^-5 secondi) si ricorre ad uno specifico temporizzatore detto **CTC**, tipico di ogni PC. Quello, insomma, che aggiorna anche l'orologio di sistema, e grazie al quale si raggiunge una risoluzione di circa 55microsecondi (che non è poco!). Possiede una porta di controllo alla locazione **0x43** su tre canali contatori, rispettivamente a **0x40**, **0x41** e **0x42**.

CONTENUTI EXTRA!

Nella sezione Contenuti Extra, dentro alla Secret Zone del nostro sito (www.hackerjournal.it), troverete il codice sorgente del programma, pronto per essere compilato, e link utili per scaricare emulatori di Commodore 64 per le varie piattaforme. Potete accedere alla Secret Zone con le password che trovate a pagina 3 di questo numero, o dei numeri successivi).

Andando a scrivere un byte in **0x43** settiamo il **CTC** nel modo di funzionamento voluto e possiamo quindi andare a leggere per esempio in **0x40** l'attuale stato (valore) del rispettivo canale. Siccome tale valore in 0x40 viene decrementato di uno ogni tot microsecondi (se impostiamo un divisore di **65536** abbiamo un decremento ogni 55 microsecondi), leggendo lo stato del canale prima di un certo evento e dopo lo stesso evento, siamo in grado di misurare la durata di tale evento con grande precisione.
Il programma in questione non fa null'altro che **leggere in continuazione alla locazione 0x379** (ovvero l'indirizzo del registro di stato della prima parallela) e **verifica lo stato del bit7** corrispondente al pin 2 sulla porta, ovvero dove abbiamo collegato l'uscita del registratore, e controlla il tempo durante il quale tale bit vale 0 e poi 1, salvando il risultato in un buffer sufficientemente ampio. Nel frattempo, **controlla anche per il bit6**, corrispondente allo stato del pulsante play e fintanto che rimane 0 (tasto premuto) si continua a registrare. Dopodiché, si rilegge il buffer, si convertono i valori con la formula e si salva il tutto nel file out.TAP.

Il tutto si compila tranquillamente col compilatore **DJGPP (www.delorie.com/djgpp/)**. È necessario inoltre avere nella stessa directory dell'eseguibile anche un gestore per la memoria estesa (tipo **CWSDPMI.EXE**) scaricabile un po' ovunque, dato che il programma fa uso di molta memoria (4Mbyte di default). Inoltre, **gira correttamente solo in**

modalità DOS reale, in quanto non ha alcun senso misurare intervalli di tempo tanto brevi sotto un sistema multitasking dove esiste uno scheduler che stoppa e riavvia i programmi un po' quando gli pare e piace. L'unico inconveniente del programma è che non **si ha alcun output visivo durante la fase di caricamento**, e quindi non c'è modo di sapere quando i dati su nastro sono effettivamente terminati.

>> La funzione record

La funzione **record** esegue dapprima un ciclo vuoto (primo while) affinché si sincronizzi (in quanto non si può dare per scontato che si parta con un livello logico basso), dopodiché si inizializza il CTC e si aspetta per tutta la durata di 0 e di 1, verificando sempre nel frattempo che non sia scattato l'overflow (quando il CTC ha raggiunto valori troppo bassi). Successivamente si memorizza il risultato nel buffer e, se **flag** è stata settata, significa che abbiamo incontrato un overflow in almeno uno dei due cicli e quindi si memorizza un valore simbolico particolarmente basso, ovvero **0x00**.

>> La funzione buildTAP

La seguente funzione costruisce il file TAP semplicemente convertendo i valori contenuti nel buffer secondo la formula ricavata in precedenza. Siccome il buffer ha un numero di valori memorizzati pari a (**cont**), anche il ciclo for verrà effettuato (**cont**) volte. Da notare che nella formula vi è una divisione per **CTC_BASEFREQ** che non era presente in precedenza; tale divisione è necessaria in quanto il buffer non memorizza in ogni cella direttamente il tempo in secondi di ogni pulsazione, ma il numero a cui e' arrivato il CTC a contare partendo da 65536. Per esempio, se **buffer[31]** contiene il valore 65010, significa che il CTC ha effettuato nel tempo di una pulsazione ben 65536 - 65010 = 526 decrementi. Quindi la quantità in secondi è rappresentata dall'espressione: **(65536-buffer[cont]) / CTC_BASEFREQ**. Nelle prime righe della funzione si inserisce semplicemente l'header del file TAP.

>> La funzione main

Main si preoccupa di creare il buffer e il file **out.tap**, dopodiché si mette

The Winter Consumer Electronics Show

COMPUTE!'s GAZETTE

$2.50 April 1984 Issue 10 Vol. 2, No. 4

For Owners And Users Of Commodore VIC-20 And 64 Personal Computers

CALENDAR MAKING

Make any of four impressive calendars with your VIC or 64 and printer.

ROBOTS: The New Mobile Computers

Robots on the market and in the home. An inside look at what they do, what they cost, and what to look for in the years ahead.

Power BASIC: Numeric Keypad

Turn your VIC or 64 keyboard into an efficient numeric keypad with this machine language program.

NEVETS

An exciting action-strategy game for the VIC and 64.

Also In This Issue

How To Start A User Group

French Tutor

Little Known BASIC Commands

Adding A Second Joystick To The VIC

Aprile 1984, Compute! Gazette pubblica un "eccitante" gioco per Vic20 e C64, con la grafica costruita usando i caratteri ASCII. Che tempi!

in attesa del tasto play verificando il solito **bit6** in **0x379** (se risulta già premuto, avvisa di premere prima il tasto stop). Da qui in poi si chiama prima la **record()** e poi la **buildTAP()**. Infine si dealloca il buffer e si chiude il file.

Gianluca Ghettini

LINK UTILI:

http://www.devili.iki.fi/Computers/Commodore/
http://ftp.funet.fi/pub/mirrors/ftp.simtel.net/pub/simtelnet/msdos/info/pctim003.zip
http://www.geocities.com/SiliconValley/Platform/8224/c64tape/

Guestbook!

"Cosa ne pensi di Matrix Reloaded? E' all'altezza del primo film?"

Secondo me Matrix Reloaded è il film più mitico di tutti ed è completamente all'altezza del primo film, secondo me è come l'inno nazionale degli hackers di tutto il mondo (Neox) • Una vera americanata. Sembra quasi che tutti i richiami filosofici del primo film siano pura casualità. Da non vedere (Kasgor) • Matrix Reloaded é un grande guazzabuglio di personaggi forzatamente fighi ed effetti speciali...ma é Matrix Reloaded! (Zoten) • Mi puzza troppo di operazione commerciale, il primo e unico Matrix non ha niente a che fare con questo bel filmetto x ragazzini. Matrix è un cult (o), non meritava di finire così. Venduto x_4_$. (Giaipur) • "Sfortunatamente, non è possibile spiegare a parole cos'è Matrix. Devi vederlo con i tuoi occhi… (Cloud Strife) • IL 2° film è troppo stracciato... nel senso che hanno voluto far troppo con gli effetti speciali, rendendo così il film in una americanata come al solito! hanno esagerato un po' tropppo! (mat teo) • Matrix reloded è uno spettacolo..storia intenza ed affascinante che t lascia col fiato sospeso dall'inizio alla fine (recitazione della bellucci a parte) (MrZANO) • Matrix è un evento, l'idea di un leggenda. Matrix Reloaded è qualcosa costruita su un mito avendo a disposizione soldi e fama... poteva essere meglio (J3X) • Secondo me Matrix Reloaded è un film con degli effetti speciali incredibili, ma, Matrix 1 da molta più suspense e più storia di Reloaded ([C]elso) • Secondo me la trama è decisamente migliore nel primo film. Matrix Reloaded ha una trama inconsistente ma questa pecca è compensata da effetti speciali straordinari. Da non perdere!!! (Mikispag) • MR è un film troppo fico ma forse non all'altezza del 1 (_= The Disk =_) • Di MATRIX ce ne 1 tutti gli altri son NESSUNO! (CICOMTX) • Per noi è più bello del primo. La trama si infittisce e gli effetti speciali sono più spettacolari (IsaGer) • "Causa, effetto. Bevo troppo vino, devo andare in bagno". The Matrix ruulezzz! Ochèi, più scene d'azione, tuttavia riflessivo, basta andare un po' in profondità. E gli Animatrix sono grandiosi (NoWhereMan) • Non credo che basti ricaricare per portare avanti un opera gia ben congegnata.... si attendono rivoluzioni!!! (AlexSk8) • Matrix è la più grande saga cyber-punk mai concepita.Il secondo episodio secondo me è semplicemente perfetto.Da antologia il discorso con "L'Architetto"! (.::Angel::.) • Trama pretestuosa, Bellucci orribile, scene favolose di inseguimenti, meglio il primo!! Ci ha fatto sognare,Reloaded ci ha delusi… Hasta la baldoria siempre!! (Sacha Dimitri) • Penso che sia un gran Film (da vedere), ottimi effetti speciali.... magnifico. Inoltre c'è da precisare una cosa: Matrix reloaded è un film che si segue con il cuore, le pistole, le armi ecc. sono solo un diversivo! (Giovo) • Di solito i primi Film sono i migliori, ed anche in questo caso Matrix è sicuramente meglio del Reloaded dove i combattimenti sono un pò troppo lunghi, per non parlare del finale....aspettiamo Matrix3.. (ALIENz) • Io sono un Big Fan di Matrix e posso assicurarvi che è all'altezza del primo Film… Dico solo una cosa: continuate a seguire il Coniglio Bianco (Fit)

Sui prossimi numeri...

Ecco l'argomento su cui potete scatenarvi:

Chi è il tuo vero nemico?

Rispondete con una decina di parole, scrivendo a:

guestbook@hackerjournal.it